

著作権保護システム

著作権保護システム、鍵生成装置、記録装置、再生装置、読み出し装置、復号装置、記録媒体、記録方法、再生方法、及びプログラム

5

技術分野

本発明は、映画や音楽などの著作物をデジタル化したコンテンツを、光ディスク等の大容量記録媒体に記録して、再生するシステムに関し、特にコンテンツの著作権の許可なく不正利用されることを防止する著作権

10 保護システムに関する。

背景技術

近年、記録媒体が大容量化するに従い、映画や音楽などの著作物をデジタル化したコンテンツを例えば光ディスク等の記録媒体に格納して市

15 販するビジネスが盛んに行われている。

記録媒体に記録されたコンテンツは、不正にコピーされる可能性があるため、何らかの保護が必要である。

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピー等といった不正利用を防止するために暗号化技術が

20 用いられる。

具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号し、コンテンツの再生等を行うことができる。

25 なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化

して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法とがある。

このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析によって、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する再生装置あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを実現する技術を鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献1（特開2002-281013号公報）が開示されている。

一方、記録媒体に記録された暗号化コンテンツを再生する装置としては、記録媒体から暗号化コンテンツを読み出す機能と読み出した暗号化コンテンツを復号する機能が一体となったいわゆる民生用プレーヤや、パソコンに接続もしくは内蔵された光ディスクドライブで記録媒体から暗号化コンテンツを読み出し、読み出した暗号化コンテンツをパソコンのホスト上で動作するアプリケーションプログラムによって復号して再生するものがある。これら2つの種類の再生装置に対応する著作権保護システムとして、非特許文献1（Content Protection for Pre-recorded Media DVD Book、4C Entity, LLC）が公開されている。

しかしながら、上記したような従来の著作権保護システムでは、対象とするすべての種類の再生装置に対して共通の無効化データを記録媒体に記録するようにしているため、各再生装置はその無効化データ全体を記録媒体から読み込んで少なくとも一時的に格納するメモリを装置内に

設ける必要がある。

また、一般にDVDプレーヤ等の民生用プレーヤにおいては、装置に組み込まれた処理アルゴリズムや鍵の長さを変更することは、時間と手間がかかり困難である。

- 5 一方、パソコン上のアプリケーションプログラムとして復号処理や鍵がソフトウェアで実装される場合は、一般的にハードウェアで実装する場合に比べて、内蔵する復号アルゴリズムや鍵の更新や追加は容易であるが、復号アルゴリズムや鍵の堅牢な実装は困難である。しかしながら、従来の共通の無効化データを記録媒体に記録する著作権保護システムで
- 10 は、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合であっても、暗号化・復号のアルゴリズムや鍵長を変更することは実質上不可能となっている。これは、無効化機能が正しく働かなくなることを意味し、不正機器によりコンテンツの不正利用が蔓延することにつながる。また、パ
- 15 ソコンで使用されるアプリケーションの鍵やアルゴリズムが一旦暴露された場合においては、これが民生機器に及んで全ての機器において適切に無効化機能が働かなくなるような場合も考えられる。

- 本発明では、上記課題を解決するために、再生装置内に設けるメモリのサイズを小さくでき、かつ、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露
- 20 された場合でも、暗号化・復号のアルゴリズムや鍵長を変更することでシステム全体の無効化機能を維持することのできる著作権保護システムを提供する。

25 発明の開示

本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化

コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前記再生装置は N 個（ N は2以上の自然数）のカテゴリに分類されており、前記記録装置は、メディア鍵と前記 N 個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記 N 個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記 N 個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記 N 個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記 N 個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、前記各カテゴリの再生装置は、
5 前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで
10 前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記N個のメディア鍵で暗号化してN個の暗号化コンテンツ鍵を生成し、少なくとも前記N個の暗号化メディア鍵データと前記N個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体
15 に記録し、前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記
20 対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記再生装置は、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第
25 2のカテゴリに属する第2再生装置、及び前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第2のカテ

ゴリの読み出し装置と前記第 2 のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第 1 のカテゴリの復号装置とから構成される第 1 再生装置とから成り、前記記録装置は、メディア鍵と前記第 1 のカテゴリの復号装置が保有するデバイス鍵データとから

5 前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データを生成し、前記メディア鍵と前記第 2 のカテゴリの装置が保有するデバイス鍵データとから前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を

10 施した暗号化コンテンツを生成し、少なくとも前記第 1 の無効化データ、前記第 2 の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、前記第 2 再生装置は、前記記録媒体から前記第 2 の無効化データ及び前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づいて前記暗号化コンテンツを復号し、前記第 1 再生装置において、前記

15 第 2 のカテゴリの読み出し装置は、前記記録媒体から前記第 1 の無効化データ、前記第 2 の無効化データ及び前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第 1 の無効化データを前記第 1 カテゴリの復号装置に供給し、前記第 1 のカテゴリの復号装置は、前記第 2 の

20 カテゴリの読み出し装置から供給される前記中間データに前記第 1 の無効化データに基づいて復号処理を施し前記コンテンツを取得することを特徴とする。

また、本発明は、コンテンツを暗号化して記録する記録装置であって、前記記録装置は、メディア鍵と N 個 (N は 2 以上の自然数) のカテゴリ

25 に分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化

するための無効化データを前記N個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

- 5 また、本発明は、前記記録装置であって、前記N個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

また、前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする。

- 10 また、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする。

- また、本発明は、前記記録装置であって、前記N個の各無効化データ
15 は、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記N個のメディア鍵で暗号化してN個の暗号化コンテンツ鍵データを生成し、少なくとも前記N個の暗号化メディア鍵データと前記N個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体
20 に記録することを特徴とする。

- また、前記記録装置は、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データを生成し、
25 前記メディア鍵と前記第2のカテゴリの装置が保有するデバイス鍵データとから前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効

化するための第2の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

- 5 また、本発明は、暗号化コンテンツが記録される記録媒体であって、前記記録媒体には、少なくとも、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツが記録される
- 10 ことを特徴とする。

また、本発明は、前記記録媒体であって、前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

- 15 また、本発明は、前記記録媒体であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであることを特徴とする。

- また、本発明は、前記記録媒体であって、前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記
- 20 記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されることを特徴とする。

- また、本発明は、前記記録媒体であって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データで
- 25 あり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記コンテンツ鍵を

前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵が記録されることを特徴とする。

また、前記記録媒体には、少なくともメディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとが記録されることを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、前記記録媒体には、少なくともメディア鍵と前記N個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記記録媒体から前記N個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵デー

タを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを
5 暗号化して生成されたものであり、

前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記暗号化コンテンツは、コン
10 テンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテ
15 ンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して
20 生成されたものであり、前記記録媒体には、前記コンテンツ鍵を前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号
25 化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コ

ンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記第２のカテゴリに属し、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記読み出し装置は、前記第２のカテゴリに属し、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第

1の無効化データを出力することを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、前記記録媒体には、少なくともメディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記第2のカテゴリの読み出し装置は、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第1の無効化データを出力し、前記復号装置は、前記第1のカテゴリに属し、前記第2のカテゴリの読み出し装置から供給される前記中間データに前記第1の無効化データに基づいて復号処理を施して前記コンテンツを取得することを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、請求項25記載の読み取り装置と請求項26記載の復号装置とから構成されることを特徴とする。

また、本発明は、コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前

記記録装置及び前記再生装置は N 個（ N は2以上の自然数）のカテゴリに分類されており、前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記 N 個の各カテゴリに対してそれぞれ生成し、生成した前記 N 個の無効化データを前記記録媒体に記録し、前記記録装置は、前記記録媒体から前記 N 個の無効化データのうち、前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記 N 個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、鍵生成装置であって、メディア鍵と N 個（ N は2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記 N 個の各カテゴリに対してそれぞれ生成し、生成した前記 N 個の無効化データを前記記録媒体に記録することを特徴とする。

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵と N 個（ N は2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録

媒体から、前記N個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

5 また、本発明は、コンテンツを暗号化して記録する記録装置に用いる記録方法であって、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記N個の各カテゴリに対してそれぞれ生成する生成ステップと、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、
10 少なくとも前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含むことを特徴とする。

 また、本発明は、記録媒体に記録された暗号化コンテンツを再生する
15 再生装置に用いる再生方法であって、前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、前記記録媒体には、少なくともメディア鍵と前記N個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいて
20 コンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記再生方法は、前記記録媒体から前記N個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、前記読み出しステップにおいて読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する
25 復号ステップとを含むことを特徴とする。

 また、本発明は、コンテンツを暗号化して記録する記録装置に用いる

プログラムであって、メディア鍵と N 個（ N は2以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記 N 個の各カテゴリに対してそれぞれ生成する生成ステップと、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、少なくとも前記 N 個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含むことを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置に用いるプログラムであって、前記再生装置は N 個（ N は2以上の自然数）のカテゴリに分類されており、前記記録媒体には、少なくともメディア鍵と前記 N 個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記プログラムは、前記記録媒体から前記 N 個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、前記読み出しステップにおいて読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する復号ステップとを含むことを特徴とする。

図面の簡単な説明

図1は、本発明の実施の形態1における記録装置及び記録媒体を示すブロック図である。

図2は、本発明の実施の形態1における記録媒体及び第1のカテゴリの再生装置を示すブロック図である。

図 3 は、本発明の実施の形態 1 における記録媒体及び第 2 のカテゴリの再生装置を示すブロック図である。

図 4 は、本発明の実施の形態 1 における記録媒体に記録するデータ的具体例を示す模式図である。

5 図 5 は、本発明の実施の形態 1 におけるシステム更新の具体例 1 を示す模式図である。

図 6 は、本発明の実施の形態 1 におけるシステム更新の具体例 2 を示す模式図である。

10 図 7 は、本発明の実施の形態 2 における鍵生成装置及び記録媒体を示すブロック図である。

図 8 は、本発明の実施の形態 2 における第 1 のカテゴリの記録装置及び記録媒体を示すブロック図である。

図 9 は、本発明の実施の形態 2 における第 2 のカテゴリの記録装置及び記録媒体を示すブロック図である。

15 図 10 は、本発明の実施の形態 2 における記録媒体及び第 1 のカテゴリの再生装置を示すブロック図である。

図 11 は、本発明の実施の形態 2 における記録媒体及び第 2 のカテゴリの再生装置を示すブロック図である。

20 図 12 は、本発明の実施の形態 2 における記録媒体に記録するデータの具体例を示す模式図である。

図 13 は、本発明の実施の形態 3 における記録装置及び記録媒体を示すブロック図である。

図 14 は、本発明の実施の形態 3 における記録媒体及び第 1 のカテゴリの再生装置を示すブロック図である。

25 図 15 は、本発明の実施の形態 3 における記録媒体及び第 2 の再生装置を示すブロック図である。

図 1 6 は、本発明の実施の形態 3 における記録媒体に記録するデータの具体例を示す模式図である。

図 1 7 は、本発明の実施の形態 3 におけるシステム更新の具体例 1 を示す模式図である。

5 図 1 8 は、本発明の実施の形態 3 におけるシステム更新の具体例 2 を示す模式図である。

図 1 9 は、本発明の実施の形態 4 における記録装置及び記録媒体を示すブロック図である。

10 図 2 0 は、本発明の実施の形態 4 における記録媒体及び第 1 の再生装置を示すブロック図である。

図 2 1 は、本発明の実施の形態 4 における記録媒体及び第 2 の再生装置を示すブロック図である。

図 2 2 は、本発明の実施の形態 4 における記録媒体に記録するデータの具体例を示す模式図である。

15 図 2 3 は、本発明の実施の形態 4 におけるシステム更新の具体例 1 を示す模式図である。

図 2 4 は、本発明の実施の形態 4 におけるシステム更新の具体例 2 を示す模式図である。

20 図 2 5 は、本発明の実施の形態 5 における記録装置及び記録媒体を示すブロック図である。

図 2 6 は、本発明の実施の形態 5 における記録媒体及び第 1 の再生装置を示すブロック図である。

図 2 7 は、本発明の実施の形態 5 における記録媒体及び第 2 の再生装置を示すブロック図である。

25 図 2 8 は、本発明の実施の形態 5 における記録媒体に記録するデータの具体例を示す模式図である。

図 29 は、本発明の実施の形態 5 におけるシステム更新の具体例 1 を示す模式図である。

図 30 は、本発明の実施の形態 5 におけるシステム更新の具体例 2 を示す模式図である。

5 図 31 は、本発明の実施の形態 6 における記録装置及び記録媒体を示すブロック図である。

図 32 は、本発明の実施の形態 6 における記録媒体及び第 1 の再生装置を示すブロック図である。

10 図 33 は、本発明の実施の形態 6 における記録媒体及び第 2 の再生装置を示すブロック図である。

図 34 は、本発明の実施の形態 6 における記録媒体に記録するデータの具体例を示す模式図である。

図 35 は、本発明の実施の形態 6 におけるシステム更新の具体例 1 を示す模式図である。

15 図 36 は、本発明の実施の形態 6 におけるシステム更新の具体例 2 を示す模式図である。

図 37 は、本発明の実施の形態 7 における記録装置及び記録媒体を示すブロック図である。

20 図 38 は、本発明の実施の形態 7 における記録媒体及び第 1 の再生装置を示すブロック図である。

図 39 は、本発明の実施の形態 7 における記録媒体及び第 2 の再生装置を示すブロック図である。

図 40 は、本発明の実施の形態 7 における記録媒体に記録するデータの具体例を示す模式図である。

25 図 41 は、本発明の実施の形態 7 におけるシステム更新の具体例 1 を示す模式図である。

図 4 2 は、本発明の実施の形態 7 におけるシステム更新の具体例 2 を示す模式図である。

発明を実施するための最良の形態

5 以下、本発明の実施の形態について、図面を参照しながら説明する。

(実施の形態 1)

本発明の実施の形態 1 は、再生専用の DVD 等の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。尚、本実施の形態 1 においては、再生装置側に
10 第 1 及び第 2 のカテゴリを設けて、カテゴリ毎に異なるデバイス鍵を用いて無効化を行う。このため、同一の記録媒体に用いる無効化システムを再生装置側のカテゴリにより分類でき、たとえ一方の無効化システムが破られた場合においても、他のカテゴリに属する無効化システムは維持できることを特徴とする。

15 以下、本発明の実施の形態 1 について、図面を参照しながら説明する。
図 1 は、コンテンツを暗号化して記録する記録装置 100 及び記録媒体 120 を示しており、図 2 は、記録媒体 120 から暗号化コンテンツを読み出して復号する第 1 のカテゴリの再生装置 200 を示しており、図
3 は、記録媒体 120 から暗号化コンテンツを読み出して復号する第 2
20 のカテゴリの再生装置 300 を示している。また、図 4 は記録媒体 120 に記録される各種データの具体例を示している。

記録装置 100 は、例えば、製造時において各 DVD にコンテンツを記録するような装置であり、第 1 のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第 1 のデバイス鍵格納部 101 と、第 2 のカ
25 テゴリの各再生装置が秘密に保有するデバイス鍵を格納する第 2 のデバイス鍵格納部 102 と、メディア鍵を暗号化するために用いるデバイス

鍵を選択する第１のデバイス鍵選択部１０３及び第２のデバイス鍵選択部１０４と、外部から入力されるメディア鍵を第１のデバイス鍵選択部１０３で選択したデバイス鍵で暗号化する第１のメディア鍵暗号化部１０５と、メディア鍵を第２のデバイス鍵選択部１０４で選択したデバイス鍵で暗号化する第２のメディア鍵暗号化部１０６と、外部から入力されるコンテンツ鍵をメディア鍵で暗号化するコンテンツ鍵暗号化部１０７と、同じく外部から入力されるコンテンツを暗号化するコンテンツ暗号化部１０８とを備える。

なお、図１には示していないが、第１のメディア鍵暗号化部１０５には、第１のカテゴリの再生装置のうち無効化すべき再生装置の情報が、第２のメディア鍵暗号化部１０６には第２のカテゴリの再生装置のうち無効化すべき再生装置の情報が、それぞれ入力されており、暗号化メディア鍵を生成する際にこれら無効化すべき再生装置では正しいメディア鍵が復号できないように暗号化メディア鍵を生成する。さらにメディア鍵は記録媒体を製造する度に、コンテンツ鍵はコンテンツ毎に異なる鍵データを選択している。

記録媒体１２０は、第１のメディア鍵暗号化部１０５が生成した第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１２１と、第２のメディア鍵暗号化部１０６が生成した第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１２２と、コンテンツ鍵暗号化部１０７が生成した暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域１２３と、コンテンツ暗号化部１０８が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１２４とを備える。

第１のカテゴリの再生装置２００は、デバイス鍵を秘密に保有するデバイス鍵格納部２０１と、デバイス鍵を用いて記録媒体１２０から読み

出した第 1 の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部 202 と、取得したメディア鍵を用いて記録媒体 120 から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部 203 と、取得したコンテンツ鍵を用いて記録媒体 120 から読み出した暗号化コンテンツを復号するコンテンツ復号部 204 とを備える。本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される再生装置を第 1 のカテゴリに属する再生装置とした。

第 2 のカテゴリの再生装置 300 は、デバイス鍵を秘密に保有するデバイス鍵格納部 301 と、デバイス鍵を用いて記録媒体 120 から読み出した第 2 の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部 302 と、取得したメディア鍵を用いて記録媒体 120 から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部 303 と、取得したコンテンツ鍵を用いて記録媒体 120 から読み出した暗号化コンテンツを復号するコンテンツ復号部 304 とを備える。本実施の形態では一般的な民生プレーヤのようにハードウェアで実装される再生装置を第 2 のカテゴリに属する再生装置とした。

図 4 は、 m 台の第 1 のカテゴリの再生装置及び n 台の第 2 のカテゴリの再生装置がそれぞれ固有のデバイス鍵を 1 個だけ保有しており、第 1 のカテゴリの再生装置 2 と第 2 のカテゴリの再生装置 3 が無効化されているとした場合の、記録媒体 120 に記録される各種データの具体例を示している。図 4 中で、第 1 のカテゴリの再生装置 i ($i = 1 \sim m$) が保有するデバイス鍵を DKA_i 、第 2 のカテゴリの再生装置 j ($j = 1 \sim n$) が保有するデバイス鍵を DKB_j としている。また、 $E_a(X, Y)$ 、 $E_b(X, Y)$ 、 $E_c(X, Y)$ 及び $E_d(X, Y)$ はデータ Y

を鍵データXを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長56bitのDES暗号を使用した。

(第1の暗号化メディア鍵データ記録領域121)

5 第1の暗号化メディア鍵データ記録領域121には、第1のカテゴリの再生装置が保有するデバイス鍵(DKA1~DKAm)で暗号化されたメディア鍵(MK)が記録されている。ここで、第1のカテゴリの再生装置2は無効化されており、DKA2ではメディア鍵(MK)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第
10 1の暗号化メディア鍵を生成する際に、第1のメディア鍵暗号化部105において、第1のカテゴリのうち無効化すべき再生装置の情報として再生装置2が入力され、再生装置2では正しいメディア鍵が得られないように処理された結果である。

(第2の暗号化メディア鍵データ記録領域122)

15 第2の暗号化メディア鍵データ記録領域122には、第2のカテゴリの再生装置が保有するデバイス鍵(DKB1~DKBn)で暗号化されたメディア鍵(MK)が記録されている。ここで、第2のカテゴリの再生装置3は無効化されており、DKB3ではメディア鍵(MK)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第
20 2の暗号化メディア鍵を生成する際に、第2のメディア鍵暗号化部106において、第2のカテゴリのうち無効化すべき再生装置の情報として再生装置3が入力され、再生装置3では正しいメディア鍵が得られないように処理された結果である。

第1及び第2の暗号化メディア鍵データをこのように生成することにより、第1のカテゴリの再生装置2及び第2のカテゴリの再生装置3を除く再生装置が正しいメディア鍵(MK)を復号することができるのと

25

もに、第 1 のカテゴリの再生装置 2 及び第 2 のカテゴリの再生装置 3 をシステムから排除することができる。

(暗号化コンテンツ鍵記録領域 1 2 3)

5 暗号化コンテンツ鍵記録領域 1 2 3 にはメディア鍵 (MK) で暗号化されたコンテンツ鍵 (CK) が記録されている。

(暗号化コンテンツ記録領域 1 2 4)

暗号化コンテンツ記録領域 1 2 4 には、コンテンツ鍵 (CK) で暗号化されたコンテンツが記録されている。

10 以上のように構成された本発明の実施の形態 1 において、例えば第 1 のカテゴリの再生装置に付与したデバイス鍵の多数や、第 1 の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第 1 のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第 1 のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

15 (システム更新の具体例 1)

第 1 のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成される記録媒体 1 2 0 に記録する各種データの具体例 1 を図 5 に示す。図 4 との違いは、第 1 の暗号化メディア鍵データの生成に用いるデバイス鍵を DKA 1 ~ DKA m から DKA' 1 ~ DKA' m に変更したことである。ここで、新たなデバイス鍵 (DKA' 1 ~ DKA' m) のうちの各デバイス鍵は、システム更新前のデバイス鍵 (DKA 1 ~ DKA m) のどれとも一致しないようになっている。このため、無効化が機能しなくなった以後の記録媒体 1 2 0 の製造時において無効化システムを更新することが可能となる。

25 一方、無効化されていない第 1 のカテゴリの再生装置 2 0 0 には、新たなデバイス鍵が付与され、デバイス鍵格納部 2 0 1 に格納される。例

例えば、第 1 のカテゴリの再生装置 m は、以前から保有していたデバイス鍵 (DKA_m) に加え、新たに付与されたデバイス鍵 (DKA'_m) をデバイス鍵格納部 201 に保有する。再生装置 m は、図 4 の記録媒体を再生する際には、デバイス鍵 DKA_m を用い、無効化システム更新後の
5 図 5 の記録媒体を再生する際には、デバイス鍵 DKA'_m を用いて、記録媒体から読み出した第 1 の暗号化メディア鍵を復号してメディア鍵 (MK) を取得し、取得したメディア鍵 (MK) を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵 (CK) を取得し、取得したコンテンツ鍵 (CK) を用いて暗号化コンテンツを復号再生する。

10 ここで、新たなデバイス鍵 ($DKA'_1 \sim DKA'_m$) のうちの各デバイス鍵は、システム更新前のデバイス鍵 ($DKA_1 \sim DKA_m$) のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が DKA_2 以外に存在したとしても、そのデバイス鍵を使って図 5 の記録媒体から読み出した第 1 の暗号化メ
15 ディア鍵を復号してメディア鍵 (MK) を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第 2 の暗号化メディア鍵データの生成に用いるデバイス鍵 ($DKB_1 \sim DKB_n$) は変更されていないので、第 2 のカテゴリに属する再生装置には何らの変更を加える必要
20 がない。

(システム更新の具体例 2)

第 1 のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成される記録媒体 120 に記録する各種データの具体例 2 を図 6 に示す。図 4 との違いは、第 1 の暗号化メディア鍵の生成に用
25 いるデバイス鍵を $DKA_1 \sim DKA_m$ から $DKA'_1 \sim DKA'_m$ に変更したことと、暗号化アルゴリズムを $E_a(X; Y)$ から $E_{a'}(X,$

Y)に変更したことである。ここで、新たなデバイス鍵(DKA' 1 ~ DKA' m)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA 1 ~ DKA m)のどれとも一致しないようになっている。

一方、無効化されていない第1のカテゴリの各再生装置200には、
5 新たなデバイス鍵を付与されデバイス鍵格納部201に格納される。また、メディア鍵復号部202には、以前から組み込まれている図4の第1の暗号化メディア鍵データを復号するための復号アルゴリズムDa(X, Y)に加えて、図5の第1の暗号化メディア鍵データを復号するための復号アルゴリズムDa'(X, Y)が組み込まれる。例えば、第
10 1のカテゴリの再生装置mは、以前から保有していたデバイス鍵(DKA m)に加え、新たに付与されたデバイス鍵(DKA' m)を保有する。再生装置mは、図4の記録媒体を再生する際には、デバイス鍵DKA mと暗号化アルゴリズムDa(X, Y)を用い、図5の記録媒体を再生する際には、デバイス鍵DKA' mと暗号アルゴリズムDa'(X, Y)
15 を用いて、記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK)を取得し、取得したメディア鍵(MK)を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵(CK)を取得し、取得したコンテンツ鍵(CK)を用いて暗号化コンテンツを復号する。本実施の形態ではEa(X, Y)及びDa(X, Y)は鍵長56bitのDES暗号を用いたのに対して、Ea'(X, Y)及びDa'(X, Y)では2キートリプルDESと呼ばれる鍵長112bitの暗号を用いた。
20

ここで、新たなデバイス鍵(DKA' 1 ~ DKA' m)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA 1 ~ DKA m)のどれとも一致しないようになっているので、システム更新前に不正な解析
25 行為により暴露されたデバイス鍵がDKA 2以外に存在したとしても、そのデバイス鍵を使って図5の記録媒体から読み出した第1の暗号化メ

メディア鍵データを復号してメディア鍵(MK)を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵(DKB1~DKBn)及び第2の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第2のカテゴリに属する再生装置には何らの変更を加える必要がない。

10 なお、システム更新の具体例1、2ともに記録媒体にはシステム更新の世代に関する情報を記録しており、第1のカテゴリの再生装置はこの情報に基づいて、いずれの世代のデバイス鍵あるいはアルゴリズムを使用するかを判断する。

15 以上のように構成された本発明の実施の形態1によれば、第1のカテゴリの再生装置200及び第2のカテゴリの再生装置300は、それぞれ異なるカテゴリの再生装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとするこ
20 ができるため、第1のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの再生装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの再生装置に影響を与えることなく、
25 無効化システムを変更することが可能になる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易では

あるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。そして、例えば、第1カテゴリに属する再生装置は、アプリケーション
5 でコンテンツの復号を実現するPC、第2カテゴリに属する再生装置としては、ハードウェアでコンテンツの復号を実現するDVDプレーヤ等の民生機器が挙げられる。

なお、本実施の形態では図1において、メディア鍵及びコンテンツ鍵が記録装置100の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置100がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、
10 記録装置100がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

また、本実施の形態では図1において、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵をメディア鍵で暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する1階層の構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図1に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、
20 コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図1中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置さ
25

れる装置に内蔵され、コンテンツ暗号化部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図5の $E_a(DKA', 2, 0)$ や図6の $E_a(DKA', 2, 0)$ のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する再生装置の台数を増やすことが可能となる。

また、本実施の形態では、図4に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してよく、例えば特許文献1として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

(実施の形態 2)

本発明の実施の形態 2 は、書き換え型もしくは追記型の DVD-RAM や DVD-R 等の記録媒体に DVD レコーダ等の記録装置でコンテンツ鍵を用いて暗号化したコンテンツを記録し、再生装置で暗号化コンテンツをコンテンツ鍵で復号化した後に再生するシステムに本発明を適用
5 することを特徴としている。

以下、本発明の実施の形態 2 について、図面を参照しながら説明する。
図 7 は、鍵情報を生成して記録する鍵生成装置 700 及び記録媒体 720 を示しており、図 8 は、記録媒体 720 にコンテンツを暗号化して記録する第 1 のカテゴリの記録装置 800 を示しており、図 9 は、記録媒体 720 にコンテンツを暗号化して記録する第 2 のカテゴリの記録装置 900 を示しており、図 10 は記録媒体 720 から暗号化コンテンツを読み出して復号する第 1 のカテゴリの再生装置 1000 を示しており、
10 図 11 は記録媒体 720 から暗号化コンテンツを読み出して復号する第 2 のカテゴリの再生装置 1100 を示している。また、図 12 は、記録媒体 720 に記録される各種データの具体例を示している。

鍵生成装置 700 は、第 1 のデバイス鍵格納部 701 に第 1 のカテゴリの各装置が秘密に保有するデバイス鍵を、第 2 のデバイス鍵格納部 702 に第 2 のカテゴリの各装置が秘密に保有するデバイス鍵を、それぞれ格納する。メディア鍵及びコンテンツ鍵の暗号化については、前記した実施の形態 1 における記録装置と同様であるので、その説明は省略する。
20

記録媒体 720 は、第 1 の暗号化メディア鍵データ記録領域 721 と、第 2 の暗号化メディア鍵データ記録領域 722 と、暗号化コンテンツ鍵記録領域 723 と、暗号化コンテンツ記録領域 724 とを備える。ここで、
25 破線で囲んだ、第 1 の暗号化メディア鍵データ記録領域 721、第 2 の

暗号化メディア鍵データ記録領域 722、及び、暗号化コンテンツ鍵記録領域 723 は、第 1 のカテゴリの記録装置 800 及び第 2 のカテゴリの記録装置 900 では記録不可能な領域である。一方、暗号化コンテンツ記録領域は、第 1 のカテゴリの記録装置 800 及び第 2 のカテゴリの
5 記録装置 900 で記録可能な領域である。

第 1 のカテゴリの記録装置 800 は、デバイス鍵を秘密に保有するデバイス鍵格納部 801 と、デバイス鍵を用いて記録媒体 720 から読み出した第 1 の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部 802 と、取得したメディア鍵を用いて記録媒体から
10 読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部 803 と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部 804 とを備える。本実施の形態では、パソコン上のアプリケーションプログラムのようにソフトウェアで実装される記録装置を第 1 のカテゴリに属する記録装置
15 とした。

第 2 のカテゴリの記録装置 900 は、デバイス鍵を秘密に保有するデバイス鍵格納部 901 と、デバイス鍵を用いて記録媒体 720 から読み出した第 2 の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部 902 と、取得したメディア鍵を用いて記録媒体から
20 読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部 903 と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部 904 とを備える。本実施の形態では、一般的な民生レコーダのようにハードウェアで実装される記録装置を第 2 のカテゴリに属する記録装置とした。

25 第 1 のカテゴリの再生装置 1000 及び第 2 のカテゴリの再生装置 1100 は、それぞれ前記した本発明の実施の形態 1 における第 1 のカテ

ゴリの再生装置 200 及び第 2 のカテゴリの再生装置 300 と同じ構成であり、同一の構成要素には同一の符号を付し、その説明を省略する。

図 12 は、 m 台の第 1 のカテゴリの装置、及び n 台の第 2 のカテゴリの装置がそれぞれ固有のデバイス鍵を 1 個だけ保有しており、第 1 のカテゴリの装置 2 と第 2 のカテゴリの装置 3 が無効化されているとした場合の、記録媒体 720 に記録される各種データの具体例を示している。図 12 中で、第 1 のカテゴリの装置 i ($i = 1 \sim m$) が保有するデバイス鍵を DKA_i 、第 2 のカテゴリの装置 j ($j = 1 \sim n$) が保有するデバイス鍵を DKB_j としている。なお、第 1 の暗号化メディア鍵データ記録領域 721、第 2 の暗号化メディア鍵データ記録領域 722、暗号化コンテンツ鍵データ記録領域 723、及び暗号化コンテンツ記録領域 724 に記録されるデータは、それぞれ前記した本発明の実施の形態 1 における第 1 の暗号化メディア鍵データ記録領域 121、第 2 の暗号化メディア鍵データ記録領域 122、暗号化コンテンツ鍵データ記録領域 123、及び暗号化コンテンツ記録領域 124 に記録されるデータと同じであるので、その説明を省略する。

本実施の形態によれば、上記した構成により、第 1 のカテゴリの装置 2 及び第 2 のカテゴリの装置 3 を除く装置が正しいメディア鍵 (MK) を復号することができるとともに、第 1 のカテゴリの装置 2 及び第 2 のカテゴリの装置 3 をシステムから排除することができる。

また、本実施の形態において、第 1 のカテゴリの装置の無効化が機能しなくなったと判断された場合には、第 1 のカテゴリの装置の無効化システムを更新することになる。更新の方法については、前記した本発明の実施の形態 1 の場合と同様の方法がとれるので、その説明を省略する。

なお、システムの更新に際して、第 2 の暗号化メディア鍵の生成に用いるデバイス鍵 ($DKB_1 \sim DKB_n$) は変更されていないので、第 2

のカテゴリに属する記録装置及び再生装置には何らの変更を加える必要がない。

5 以上のように構成された本発明の実施の形態2によれば、第1のカテゴリの装置（記録装置800及び再生装置1000）及び第2のカテゴリの装置（記録装置900及び再生装置1100）は、それぞれ異なるカテゴリの装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、
10 第1のカテゴリの装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される装置とした場合に、特に有効である。

20 なお、本実施の形態では、各カテゴリの記録装置と再生装置が別々の装置である形態としたが、本発明はそれに限定されるものではない。例えば、記録装置と再生装置が同一の装置である形態であっても良い。

また、本実施の形態では図7において、メディア鍵及びコンテンツ鍵が鍵生成装置700の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、鍵生成装置700がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。ま
25

た、鍵生成装置 700 がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

また、本実施の形態では図 8 及び図 9 において、メディア鍵で暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得したコンテンツ鍵
5 でコンテンツを暗号化する 2 階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する 1 階層の構成であってもよい。また、記録装置内部で生成したコンテンツ鍵を用いてコンテンツを暗号化し、コンテンツ鍵をメディア鍵で暗号化し、暗号化コンテンツと暗号化コンテンツ鍵を記録媒体に記録する
10 構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では鍵生成装置として図 7 に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、及び記録媒体への各データの記録が一体の構成としたが、本発明はそれ
15 に限定されるものではない。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、記録媒体への各データの記録は記録媒体製造機関に設置される装置で実行される
20 形態であっても良い。一般的に書き換え型もしくは追記型の光ディスクでは、一般ユーザの保有する記録装置で記録可能な領域と、一般ユーザの保有する記録装置では記録不可能な再生専用領域を備えており、この再生専用領域にはディスク製造業者が出荷前にデータを記録する。この場合、ディスク製造業者による再生専用領域へのデータ記録は、スタン
25 パと呼ばれる原盤にデータを記録し、このスタンパを用いたプレス工程で行われるのが一般的である。このようなディスク製造業者による再生

専用領域へのデータ記録工程において、暗号化メディア鍵データが記録媒体に記録される場合であっても本発明は適用可能である。

(実施の形態 3)

本発明の実施の形態 3 は、実施の形態 1 と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。また、1 枚の記録媒体に対して第 1 及び第 2 の 2 つのメディア鍵を用いて、第 1 カテゴリ及び第 2 カテゴリに属する再生装置において読み込まれる無効化データを記録媒体に記録することを特徴とする。

以下、本発明の実施の形態 3 について、図面を参照にしながら説明する。図 1 3 は、コンテンツを暗号化して記録する記録装置 1 3 0 0 及び記録媒体 1 3 2 0 を示しており、図 1 4 は、記録媒体 1 3 2 0 から暗号化コンテンツを読み出して復号する第 1 のカテゴリの再生装置 1 4 0 0 を示しており、図 1 5 は、記録媒体 1 3 2 0 から暗号化コンテンツを読み出して復号する第 2 のカテゴリの再生装置 1 5 0 0 を示している。また、図 1 6 は記録媒体 1 3 2 0 に記録される各種データの具体例を示している。

図 1 3 の記録装置 1 3 0 0 が図 1 の記録装置 1 0 0 と異なる点は、第 1 のカテゴリに対しては第 1 のメディア鍵を、第 2 のカテゴリに対しては第 2 のメディア鍵を、個別に設け、第 1 及び第 2 のメディア鍵をそれぞれ第 1 のメディア鍵暗号化部 1 3 0 5 及び第 2 のメディア鍵暗号化部 1 3 0 6 で暗号化し、コンテンツ鍵を第 1 及び第 2 のメディア鍵を用いてそれぞれ第 1 のコンテンツ鍵暗号化部 1 3 0 7 及び第 2 のコンテンツ鍵暗号化部 1 3 0 8 で暗号化し、記録媒体 1 3 2 0 に記録するようにしたことである。その他の点は図 1 の記録装置 1 0 0 と同じであるので、その説明は省略する。

記録媒体 1320 は、第 1 のメディア鍵暗号化部 1305 が生成した第 1 の暗号化メディア鍵データを記録する第 1 の暗号化メディア鍵データ記録領域 1321 と、第 2 のメディア鍵暗号化部 1306 が生成した第 2 の暗号化メディア鍵データを記録する第 2 の暗号化メディア鍵データ記録領域 1322 と、第 1 のコンテンツ鍵暗号化部 1307 が生成した第 1 の暗号化コンテンツ鍵を記録する第 1 の暗号化コンテンツ鍵記録領域 1323 と、第 2 のコンテンツ鍵暗号化部 1308 が生成した第 2 の暗号化コンテンツ鍵を記録する第 2 の暗号化コンテンツ鍵記録領域 1324 と、コンテンツ暗号化部 1309 が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域 1325 とを備える。

第 1 カテゴリーの再生装置 1400 及び第 2 のカテゴリーの再生装置 1500 は、それぞれ記録媒体 1320 から読み出した第 1 および第 2 の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する。その他の点については、実施の形態 1 における第 1 のカテゴリーの再生装置 200 及び第 2 のカテゴリーの再生装置 300 と同様であるので、その説明は省略する。

図 16 は、 m 台の第 1 のカテゴリーの再生装置及び n 台の第 2 のカテゴリーの再生装置がそれぞれ固有のデバイス鍵を 1 個だけ保有しており、第 1 のカテゴリーの再生装置 2 と第 2 のカテゴリーの再生装置 3 が無効化されているとした場合の、記録媒体 1320 に記録される各種データの具体例を示している。図 16 中で、第 1 のカテゴリーの再生装置 i ($i = 1 \sim m$) が保有するデバイス鍵を DKA_i 、第 2 のカテゴリーの再生装置 j ($j = 1 \sim n$) が保有するデバイス鍵を DKB_j としている。また、 $E_a(X, Y)$ 、 $E_b(X, Y)$ 、 $E_c(X, Y)$ 、 $E_d(X, Y)$ 及び $E_e(X, Y)$ はデータ Y を鍵データ X を用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長 56 bit の DES 暗号を使用した。

(第1の暗号化メディア鍵データ記録領域1321)

第1の暗号化メディア鍵データ記録領域1321には、第1のカテゴリの再生装置が保有するデバイス鍵(DKA1~DKAm)で暗号化された第1のメディア鍵(MK1)が記録されている。ここで、第1のカテゴリの再生装置2は無効化されており、DKA2では第1のメディア鍵(MK1)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第1の暗号化メディア鍵データを生成する際に、第1のメディア鍵暗号化部1305において、第1のカテゴリのうち無効化すべき再生装置の情報として再生装置2が入力され、再生装置2では正しいメディア鍵が得られないように処理された結果である。第1の暗号化メディア鍵データをこのように生成することにより、再生装置2を除く第1のカテゴリの再生装置が正しい第1のメディア鍵(MK1)を復号することができ、再生装置2をシステムから排除することができる。

(第2の暗号化メディア鍵データ記録領域1322)

第2の暗号化メディア鍵データ記録領域1322には、第2のカテゴリの再生装置が保有するデバイス鍵(DKB1~DKBn)で暗号化された第2のメディア鍵(MK2)が記録されている。ここで、第2のカテゴリの再生装置3は無効化されており、DKB3では第2のメディア鍵(MK2)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第2の暗号化メディア鍵データを生成する際に、第2のメディア鍵暗号化部1306において、第2のカテゴリのうち無効化すべき再生装置の情報として再生装置3が入力され、再生装置3では正しいメディア鍵が得られないように処理された結果である。第2の暗号化メディア鍵データをこのように生成することにより、再生装置3を除く第2のカテゴリの再生装置が正しい第2のメディア鍵(MK2)を復号することができ、再生装置3をシステムから排除することができる。

(第1の暗号化コンテンツ鍵記録領域1323)

第1の暗号化コンテンツ鍵記録領域1323には第1のメディア鍵(MK1)で暗号化されたコンテンツ鍵(CK)が記録されている。

(第2の暗号化コンテンツ鍵記録領域1324)

5 第2の暗号化コンテンツ鍵データ記録領域1324には第2のメディア鍵(MK2)で暗号化されたコンテンツ鍵(CK)が記録されている。

(暗号化コンテンツ記録領域1325)

暗号化コンテンツ記録領域1325には、コンテンツ鍵(CK)で暗号化されたコンテンツが記録されている。

10 以上のように構成された本発明の実施の形態1において、例えば第1のカテゴリの再生装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵及び第1の暗号化コンテンツ鍵を復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの再生装置の無効化が機能しなくなると判断された場合には、第1のカテゴリの再生装置の
15 無効化システムを更新することになる。以下、その具体例を説明する。

(システム更新の具体例1)

第1のカテゴリの再生装置の無効化が機能しなくなると判断されて以降、新たに作成する記録媒体1320に記録する各種データの具体例1を図17に示す。図16との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1～DKAmからDKA'1～DKA'mに変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例1と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵(DKA'1～DKA'm)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA1～DKAm)のどれとも一致しないようになっているので、システム更新前に不正な解析
25

行為により暴露されたデバイス鍵がDKA 2以外に存在したとしても、そのデバイス鍵を使って図17の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK 1)を取得することはできず、コンテンツを再生することはできない。

- 5 なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵(DKB 1~DKB n)は変更されていないので、第2のカテゴリに属する再生装置には何らの変更を加える必要がない。

(システム更新の具体例2)

- 10 第1のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体1320に記録する各種データの具体例2を図18に示す。図16との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA 1~DKA mからDKA' 1~DKA' mに変更したこと、第1の暗号化メディア鍵データの暗号化アルゴリズムをEa(X, Y)からEa'(X, Y)に変更したこと、第1の暗号化コンテンツ鍵の暗号化アルゴリズムをEc(X, Y)からEc'(X, Y)に変更したことである。ここで、新たなデバイス鍵(DKA' 1~DKA' m)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA 1~DKA m)のどれとも一致しないようになっている。
- 15 一方、無効化されていない第1のカテゴリの各再生装置1400には、新たなデバイス鍵を付与されデバイス鍵格納部1401に格納される。メディア鍵復号部1402には、以前から組み込まれている図16の第1の暗号化メディア鍵を復号するための復号アルゴリズムDa(X, Y)に加えて、図18の第1の暗号化メディア鍵を復号するための復号アルゴリズムDa'(X, Y)が組み込まれる。また、コンテンツ鍵復号部
- 20 1403には、以前から組み込まれている図16の第1の暗号化コンテ
- 25

コンテンツ鍵を復号するための復号アルゴリズム $D_c(X, Y)$ に加えて、図 18 の第 1 の暗号化コンテンツ鍵を復号するための復号アルゴリズム $D_{c'}(X, Y)$ が組み込まれる。例えば、第 1 のカテゴリの再生装置 m は、以前から保有していたデバイス鍵 (DKA_m) に加え、新たに付与されたデバイス鍵 (DKA'_m) を保有する。再生装置 m は、図 16 の記録媒体を再生する際には、デバイス鍵 DKA_m と暗号化アルゴリズム $D_a(X, Y)$ を用いて、第 1 の暗号化メディア鍵データを復号して第 1 のメディア鍵 (MK_1) を取得し、取得した第 1 のメディア鍵 (MK_1) と暗号化アルゴリズム $D_c(X, Y)$ を用いて第 1 の暗号化コンテンツ鍵を復号してコンテンツ鍵 (CK) を取得し、取得したコンテンツ鍵 (CK) を用いて暗号化コンテンツを復号する。一方、図 18 の記録媒体を再生する際には、デバイス鍵 DKA'_m と暗号アルゴリズム $D_{a'}(X, Y)$ を用いて、第 1 の暗号化メディア鍵データを復号してメディア鍵 (MK_1) を取得し、取得したメディア鍵 (MK_1) と暗号化アルゴリズム $D_{c'}(X, Y)$ を用いて第 1 の暗号化コンテンツ鍵を復号してコンテンツ鍵 (CK) を取得し、取得したコンテンツ鍵 (CK) を用いて暗号化コンテンツを復号する。本実施の形態では $E_a(X, Y)$ 、 $D_a(X, Y)$ 、 $E_c(X, Y)$ 及び $D_c(X, Y)$ は鍵長 56 bit の DES 暗号を用いたのに対して、 $E_{a'}(X, Y)$ 、 $D_{a'}(X, Y)$ 、 $E_{c'}(X, Y)$ 及び $D_{c'}(X, Y)$ 、では 2 キートリプル DES と呼ばれる鍵長 112 bit の暗号を用いた。

ここで、新たなデバイス鍵 ($DKA'_1 \sim DKA'_m$) のうちの各デバイス鍵は、システム更新前のデバイス鍵 ($DKA_1 \sim DKA_m$) のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が DKA_2 以外に存在したとしても、そのデバイス鍵を使って図 18 の記録媒体から読み出した第 1 の暗号化

メディア鍵データを復号してメディア鍵（MK1）を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正
5 取得するといった行為を困難にすることができる。

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵（DKB1～DKBn）、第2の暗号化メディア鍵データの暗号化アルゴリズム、及び第2の暗号化コンテンツ鍵データの暗号化アルゴリズムは変更されていないので、第2のカテゴリ
10 に属する再生装置には何らの変更を加える必要がない。

以上のように構成された本発明の実施の形態3によれば、第1のカテゴリの再生装置1400及び第2のカテゴリの再生装置1500は、それぞれ異なるカテゴリの再生装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設ける
15 メモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データ及び第1の暗号化コンテンツ鍵の生成に用いる暗号化アルゴリズムを、それぞれ第2の暗号化メディア鍵データ及び第2の暗号化コンテンツ鍵の生成に用いる暗号化アルゴリズムと異なるものとする
20 ことができるため、第1のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの再生装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。

また、本実施の形態では第1のカテゴリと第2のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を
25 設けることにより、カテゴリ間の独立性を高めることが可能となる。す

なわち第1のカテゴリに属する再生装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第1のメディア鍵のみであり、第2のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。

10 なお、図13では、第1のメディア鍵、第2のメディア鍵及びコンテンツ鍵が記録装置1300の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置1300が第1のメディア鍵、第2のメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置1300が第1のメディア鍵、第2のメディア鍵及びコンテンツ鍵をその都度生成する生成部を
15 有する構成であってもよい。

また、図13では、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を第1及び第2のメディア鍵で暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

20 また、本実施の形態では記録装置として図13に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではない。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部（図13
25 中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用す

る機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第 1 の暗号化メディア鍵データを生成する際に、図 17 の $E_a(DKA', 2, 0)$ や図 18 の $E_{a'}(DKA', 2, 0)$ のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第 1 の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第 1 のカテゴリに属する再生装置の台数を増やすことが可能となる。

また、本実施の形態では、図 16 に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献 1 として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長 56 bit の DES、あるいはシステム更新後の暗号アルゴリズムとして鍵長 112 bit の 2 キートリプル DES を用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長 128 bit の AES 等を用いても良い。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態 2 のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ
5 及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

(実施の形態 4)

10 本発明の実施の形態 4 は、実施の形態 1 と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。また、本実施の形態 4 に係る記録装置は、第 1 のコンテンツ鍵及び第 2 のコンテンツ鍵を用いてコンテンツを 2 回暗号化するものである。

15 以下、本発明の実施の形態 4 について、図面を参照にしながら説明する。図 19 は、コンテンツを暗号化して記録する記録装置 1900 及び記録媒体 1920 を示しており、図 20 は、記録媒体 1920 から暗号化コンテンツを読み出して復号する第 1 の再生装置 2000 を示しており、図 21 は、記録媒体 1920 から暗号化コンテンツを読み出して復
20 号する第 2 の再生装置 2100 を示している。また、図 22 は記録媒体 1920 に記録される各種データの具体例を示している。

図 19 の記録装置 1900 が図 1 の記録装置 100 と異なる点は、コンテンツに対して第 1 のコンテンツ鍵を用いて第 1 のコンテンツ暗号化部 1909 で第 1 のコンテンツ暗号化を施し、その出力に対して第 2 の
25 コンテンツ鍵を用いて第 2 のコンテンツ暗号化部 1910 で第 2 のコンテンツ暗号化を施し、メディア鍵を用いて第 1 及び第 2 のコンテンツ鍵

をそれぞれ第 1 のコンテンツ鍵暗号化部 1 9 0 7 及び第 2 のコンテンツ鍵暗号化部 1 9 0 8 で暗号化し、記録媒体 1 9 2 0 に記録するようにしたことである。その他の点は図 1 の記録装置 1 0 0 と同じであるので、その説明は省略する。

5 記録媒体 1 9 2 0 は、第 1 の暗号化メディア鍵データを記録する第 1 の暗号化メディア鍵データ記録領域 1 9 2 1 と、第 2 の暗号化メディア鍵データを記録する第 2 の暗号化メディア鍵データ記録領域 1 9 2 2 と、第 1 のコンテンツ鍵暗号化部 1 9 0 7 が生成した第 1 の暗号化コンテンツ鍵を記録する第 1 の暗号化コンテンツ鍵記録領域 1 9 2 3 と、第 2 の
10 コンテンツ鍵暗号化部 1 9 0 8 が生成した第 2 の暗号化コンテンツ鍵を記録する第 2 の暗号化コンテンツ鍵記録領域 1 9 2 4 と、第 2 のコンテンツ暗号化部 1 9 1 0 が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域 1 9 2 5 とを備える。

PC 等の第 1 の再生装置 2 0 0 0 は、例えばドライブ装置である読み
15 出し装置 2 0 1 0、及び、例えばアプリケーションでコンテンツの復号を実現する復号装置 2 0 2 0 から構成される。そして、本実施の形態 4 においては、ドライブ装置等の読み出し装置 2 0 1 0 においても暗号化コンテンツの復号化を行うことを特徴としている。

読み出し装置 2 0 1 0 は、デバイス鍵を秘密に保有するデバイス鍵格
20 納部 2 0 1 1 と、デバイス鍵を用いて記録媒体 1 9 2 0 から読み出した第 2 の暗号化メディア鍵データを復号してメディア鍵を取得する第 2 のメディア鍵復号部 2 0 1 2 と、取得したメディア鍵を用いて記録媒体から読み出した第 2 の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する第 2 のコンテンツ鍵復号部 2 0 1 3 と、取得したコンテンツ鍵を用
25 いて記録媒体 1 9 2 0 から読み出した暗号化コンテンツに第 2 のコンテンツ復号処理を施す第 2 のコンテンツ復号部 2 0 1 4 とを備え、第 2 の

コンテンツ復号部 2014 で暗号化コンテンツに第 2 の復号処理を施した結果の中間データを記録媒体 1920 から読み出した第 1 の暗号化メディア鍵データ及び第 1 の暗号化コンテンツ鍵とともに復号装置 2020 に供給する。本実施の形態において、読み出し装置 2010 は上記した構成要素がハードウェアで実装されており、第 2 のカテゴリに属するものとした。

復号装置 2020 は、デバイス鍵を秘密に保有するデバイス鍵格納部 2021 と、デバイス鍵を用いて読み出し装置 2010 から供給される第 1 の暗号化メディア鍵データを復号してメディア鍵を取得する第 1 のメディア鍵復号部 2022 と、取得したメディア鍵を用いて読み出し装置 2010 から供給される第 1 の暗号化コンテンツ鍵を復号して第 1 のコンテンツ鍵を取得する第 1 のコンテンツ鍵復号部 2023 と、取得した第 1 のコンテンツ鍵を用いて読み取り装置 2010 から供給される中間データに第 1 のコンテンツ復号処理を施してコンテンツを取得する第 1 のコンテンツ復号部 2024 とを備える。本実施の形態において、復号装置 2020 は上記した構成要素がソフトウェアで実装されており、第 1 のカテゴリに属するものとした。

第 2 の再生装置 2100 は、第 2 のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部 2101 と、デバイス鍵を用いて記録媒体 1920 から読み出した第 2 の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部 2102 と、取得したメディア鍵を用いて記録媒体から読み出した第 2 の暗号化コンテンツ鍵を復号して第 2 のコンテンツ鍵を取得する第 2 のコンテンツ鍵復号部 2103 と、取得した第 2 のコンテンツ鍵を用いて記録媒体 1920 から読み出した暗号化コンテンツに第 2 のコンテンツ復号処理を施す第 2 のコンテンツ復号部 2104 と、取得したメディア鍵を用いて記録媒体か

ら読み出した第1の暗号化コンテンツ鍵データを復号して第1のコンテンツ鍵を取得する第1のコンテンツ鍵復号部2105と、第2のコンテンツ復号部2104の出力に第1のコンテンツ鍵を用いて第1のコンテンツ復号処理を施してコンテンツを取得する第1のコンテンツ復号部2106とを備える。本実施の形態において、第2の再生装置2100は、上記した構成要素がハードウェアで実装されており、第2のカテゴリに属するものとした。

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第1のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光ディスクドライブのようにハードウェアで実装される装置を第2のカテゴリに属する装置とした。

図22は、 m 台の第1のカテゴリの復号装置及び n 台の第2のカテゴリの装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1のカテゴリの復号装置2と第2のカテゴリの装置3が無効化されているとした場合の、記録媒体1920に記録される各種データの具体例を示している。図22中で、第1のカテゴリの復号装置 i ($i = 1 \sim m$) が保有するデバイス鍵を DKA_i 、第2のカテゴリの装置 j ($j = 1 \sim n$) が保有するデバイス鍵を DKA_j としている。また、 $E_a(X, Y)$ 、 $E_b(X, Y)$ 、 $E_c(X, Y)$ 、 $E_d(X, Y)$ 、 $E_e(X, Y)$ 及び $E_f(X, Y)$ はデータ Y を鍵データ X を用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長56ビットのDES暗号を使用した。

第1の暗号化メディア鍵データ記録領域1921及び第2の暗号化メディア鍵データ記録領域1922に記録されるデータは、それぞれ、前記した実施の形態1における第1の暗号化メディア鍵データ記録領域1

2 1 及び第 2 の暗号化メディア鍵データ記録領域 1 2 2 に記録されるデータと同じであるので、その説明は省略する。

(第 1 の暗号化コンテンツ鍵記録領域 1 9 2 3)

第 1 の暗号化コンテンツ鍵記録領域 1 9 2 3 にはメディア鍵 (MK) 5 で暗号化された第 1 のコンテンツ鍵 (CK 1) が記録されている。

(第 2 の暗号化コンテンツ鍵記録領域 1 9 2 4)

第 2 の暗号化コンテンツ鍵記録領域 1 9 2 4 にはメディア鍵 (MK) で暗号化された第 2 のコンテンツ鍵 (CK 2) が記録されている。

(暗号化コンテンツ記録領域 1 9 2 5)

10 暗号化コンテンツ記録領域 1 9 2 5 には、第 1 のコンテンツ鍵 (CK 1) 及び第 2 のコンテンツ鍵 (CK 2) で暗号化されたコンテンツが記録されている。

以上のように構成された本発明の実施の形態 4 において、例えば第 1 のカテゴリの復号装置に付与したデバイス鍵の多数や、第 1 の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第 1 のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

(システム更新の具体例 1)

20 第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 1 9 2 0 に記録する各種データの具体例 1 を図 2 3 に示す。図 2 2 との違いは、第 1 の暗号化メディア鍵の生成に用いるデバイス鍵を DKA 1 ~ DKA m から DKA' 1 ~ DKA' m に変更したことである。これは、前記した実施の形態 1 で述べたシステム更新の具体例 1 と同様であるので、詳細についての説明は省略する。

25 ここで、新たなデバイス鍵 (DKA' 1 ~ DKA' m) のうちの各デ

パイス鍵は、システム更新前のデバイス鍵（DKA₁～DKA_m）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA₂以外に存在したとしても、そのデバイス鍵を使って図23の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵（MK）を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵（DKB₁～DKB_n）は変更されていないので、第2のカテゴリに属する装置には何らの変更を加える必要がない。

（システム更新の具体例2）

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体1920に記録する各種データの具体例2を図24に示す。図22との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA₁～DKA_mからDKA'₁～DKA'_mに変更したことと、暗号化アルゴリズムをE_a（X，Y）からE_{a'}（X，Y）に変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例2と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵（DKA'₁～DKA'_m）のうちの各デバイス鍵は、システム更新前のデバイス鍵（DKA₁～DKA_m）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA₂以外に存在したとしても、そのデバイス鍵を使って図24の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵（MK）を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

5 なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵（DKB1～DKBn）及び第2の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第2のカテゴリに属する装置には何らの変更を加える必要がない。

10 以上のように構成された本発明の実施の形態4によれば、第1のカテゴリの装置（復号装置2020）及び第2のカテゴリの装置（読み出し装置2010及び第2の再生装置2100）は、それぞれ異なるカテゴリの装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵データの生成に用
15 いる暗号化アルゴリズムと異なるものとすることができるため、第1のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの復号装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの装置に影響を与えることなく、無効化システムを変更
20 することが可能になる。さらに、第1のカテゴリの復号装置2020には、第2の暗号化コンテンツ鍵を復号するためのアルゴリズムは実装されていないので、第1のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツの復号に必要な全ての情報を取得することはできず、より堅牢な著作権保護シ
25 ステムを構築できる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難な

ソフトウェアで実装される復号装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

5 なお、図19で、メディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵が記録装置1900の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置1900がメディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置1900がメディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

10 また、図19では、コンテンツを第1及び第2のコンテンツ鍵で暗号化し、第1及び第2のコンテンツ鍵をメディア鍵で暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

15 また、本実施の形態では記録装置として図19に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、
20 メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図19中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

25 また、本実施の形態ではシステム更新において第1の暗号化メディア

鍵データを生成する際に、図 23 の $E_a(DKA', 2, 0)$ や図 24 の $E_a'(DKA', 2, 0)$ のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。

- 5 その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第 1 の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第 1 のカテゴリに属する復号装置の台数を増やすことが可能となる。

- 15 また、本実施の形態では、図 22 に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献 1 として開示されている本構造を利用した無効化方法を用いても良い。

- 20 また、本実施の形態では、暗号アルゴリズムとして鍵長 56 bit の DES、あるいはシステム更新後の暗号アルゴリズムとして鍵長 112 bit の 2 キートリプル DES を用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長 128 bit の AES 等を用いても良い。

- 25 また、図 22 では、コンテンツ全体を第 1 のコンテンツ鍵 (CK1) で暗号化した後、さらに第 2 のコンテンツ鍵 (CK2) で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第 1 のコ

コンテンツ鍵（ＣＫ１）で暗号化し、他のブロックを第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしてもよい。

5 なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体
10 を用いるシステムにも適用することができる。

（実施の形態５）

本発明の実施の形態５は、実施の形態４のシステムにおいて、第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第１の暗号化コンテンツ鍵の階層を設けるようにしたものである。
15 る。

そして、本実施の形態５においては、第１のメディア鍵及び第２のメディア鍵、第１のコンテンツ鍵及び第２のコンテンツ鍵を用いると共に、実施の形態４の再生装置２０００の構成に、新たに第２の再生装置を加えることを特徴としている。

20 以下、本発明の実施の形態５について、図面を参照しながら説明する。図２５は、コンテンツを暗号化して記録する記録装置２５００及び記録媒体２５２０を示しており、図２６は、記録媒体２５２０から暗号化コンテンツを読み出して復号する第１の再生装置２６００を示しており、図２７は、記録媒体２５２０から暗号化コンテンツを読み出して復号する第２の再生装置２７００を示している。また、図２８は記録媒体２５
25 ２０に記録される各種データの具体例を示している。

図 25 の記録装置 2500 が図 19 の記録装置 1900 と異なる点は、第 1 のカテゴリに対しては第 1 のメディア鍵を、第 2 のカテゴリに対しては第 2 のメディア鍵を、個別に設け、第 1 及び第 2 のメディア鍵をそれぞれ第 1 のメディア鍵暗号化部 2505 及び第 2 のメディア鍵暗号化部 2506 で暗号化し、第 1 のコンテンツ鍵を第 1 及び第 2 のメディア鍵を用いてそれぞれ第 1 コンテンツ鍵暗号化部 (1) 2507 及び第 1 のコンテンツ鍵暗号化部 (2) 2511 で暗号化し、記録媒体 2520 に記録するようにしたことである。その他の点については、前記した実施の形態 4 の記録装置 1900 と同じであるので、その説明は省略する。

10 記録媒体 2520 は、第 1 の暗号化メディア鍵データを記録する第 1 の暗号化メディア鍵データ記録領域 2521 と、第 2 の暗号化メディア鍵データを記録する第 2 の暗号化メディア鍵データ記録領域 2522 と、第 1 のコンテンツ鍵暗号化部 (1) 2507 が生成した第 1 の暗号化コンテンツ鍵 (1) を記録する第 1 の暗号化コンテンツ鍵 (1) 記録領域 15 2523 と、第 1 のコンテンツ鍵暗号化部 (2) 2511 が生成した第 1 の暗号化コンテンツ鍵 (2) を記録する第 1 の暗号化コンテンツ鍵 (2) 記録領域 2526 と、第 2 の暗号化コンテンツ鍵を記録する第 2 の暗号化コンテンツ鍵記録領域 2524 と、暗号化コンテンツを記録する暗号化コンテンツ記録領域 2525 とを備える。

20 第 1 の再生装置 2600 において復号装置 2620 は、読み出し装置 2610 が記録媒体 2520 から読み出した第 1 の暗号化コンテンツ鍵 (1) を復号して第 1 のコンテンツ鍵を取得する。その他の点については、前記した実施の形態 4 における第 1 の再生装置 2000 と同様であるので、その説明は省略する。

25 第 2 の再生装置 2700 は、記録媒体 2520 から読み出した第 1 の暗号化コンテンツ鍵 (2) を復号して第 1 のコンテンツ鍵を取得する。

その他の点については、前記した実施の形態 4 における第 2 の再生装置 2 1 0 0 と同様であるので、その説明は省略する。

図 2 8 は、記録媒体 2 5 2 0 に記録される各種データの具体例を示している。第 1 の暗号化メディア鍵データ記録領域 2 5 2 1 には、第 1 の
5 カテゴリの復号装置が保有するデバイス鍵 (D K A 1 ~ D K A m) で暗号化された第 1 のメディア鍵 (M K 1) が記録されており、第 2 の暗号化メディア鍵データ記録領域 2 5 2 2 には、第 2 のカテゴリの装置が保有するデバイス鍵 (D K B 1 ~ D K B m) で暗号化された第 2 のメディア鍵 (M K 2) が記録されている。また、第 1 の暗号化コンテンツ鍵 (1)
10 記録領域 2 5 2 3 には、第 1 のメディア鍵 (M K 1) で暗号化された第 1 のコンテンツ鍵 (C K 1) が記録されており、第 1 の暗号化コンテンツ鍵 (2) 記録領域 2 5 2 6 には、第 2 のメディア鍵 (M K 2) で暗号化された第 1 のコンテンツ鍵 (C K 1) が記録されている。その他の点については、前記した図 2 2 と同じであるので、説明を省略する。なお、
15 図 2 8 中の、E_g (X, Y) はデータ Y を鍵データ X を用いて暗号化する関数を意味し、本実施の形態では鍵長 5 6 ビットの D E S 暗号を使用した。

以上のように構成された本発明の実施の形態 5 において、例えば第 1 のカテゴリの復号装置に付与したデバイス鍵の多数や、第 1 の暗号化メディア鍵を復号するアルゴリズムがインターネット上で不正に公開され、
20 第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第 1 のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

(システム更新の具体例 1)

25 第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 2 5 2 0 に記録する各種データの具体例

1 を図 29 に示す。図 28 との違いは、第 1 の暗号化メディア鍵データの生成に用いるデバイス鍵を $DKA_1 \sim DKA_m$ から $DKA'_1 \sim DKA'_m$ に変更したことである。これは、前記した実施の形態 1 で述べたシステム更新の具体例 1 と同様であるので、詳細についての説明は省略する。

(システム更新の具体例 2)

第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 2520 に記録する各種データの具体例 2 を図 30 に示す。図 22 との違いは、第 1 の暗号化メディア鍵データの生成に用いるデバイス鍵を $DKA_1 \sim DKA_m$ から $DKA'_1 \sim DKA'_m$ に変更したこと、暗号化アルゴリズムを $E_a(X, Y)$ から $E_a'(X, Y)$ に変更したこと、及び第 1 の暗号化コンテンツ鍵 (1) の暗号化アルゴリズムを $E_c(X, Y)$ から $E_c'(X, Y)$ に変更したことである。これは、前記した実施の形態 3 で述べたシステム更新の具体例 2 と同様であるので、詳細についての説明は省略する。

以上のように構成された本発明の実施の形態 5 によれば、前記した実施の形態 4 同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第 1 のカテゴリと第 2 のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第 1 のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第 1 のメディア鍵のみであり、第 2 のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第 1 のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第 2 のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新

や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

5 なお、図 25 で、第 1 のメディア鍵、第 2 のメディア鍵、第 1 のコンテンツ鍵、及び第 2 のコンテンツ鍵が記録装置 2500 の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置 2500 がこれらの鍵を格納する格納部を有する構成であつてもよい。また、記録装置 2500 がこれらの鍵をその都度生成する生成部を有する構成であつてもよい。

10 また、図 25 では、コンテンツを第 1 及び第 2 のコンテンツ鍵で暗号化し、第 1 及び第 2 のコンテンツ鍵をメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であつてもよい。

15 また、本実施の形態では記録装置として図 25 に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであつても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図 25 中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であつても良い。

25 また、本実施の形態ではシステム更新において第 1 の暗号化メディア鍵データを生成する際に、図 29 の $E_a(DKA', 2, 0)$ や図 30 の $E_{a'}(DKA', 2, 0)$ のようにシステム更新の時点で無効化されて

いる復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与

5 することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する復号装置の台数を増やすことが可能となる。

10

また、本実施の形態では、図28に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献1として開示されている木構造

15 を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

20

また、図28では、コンテンツ全体を第1のコンテンツ鍵（CK1）で暗号化した後、さらに第2のコンテンツ鍵（CK2）で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第1のコンテンツ鍵（CK1）で暗号化し、他のブロックを第2のコンテンツ鍵（CK2）で暗号化するようにしてもよい。

25

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態 2 のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ
5 及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

(実施の形態 6)

10 本発明の実施の形態 6 は、実施の形態 1 と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

以下、本発明の実施の形態 6 について、図面を参照にしながら説明する。図 3 1 は、コンテンツを暗号化して記録する記録装置 3 1 0 0 及び
15 記録媒体 3 1 2 0 を示しており、図 3 2 は、記録媒体 3 1 2 0 から暗号化コンテンツを読み出して復号する第 1 の再生装置 3 2 0 0 を示しており、図 3 3 は、記録媒体 3 1 2 0 から暗号化コンテンツを読み出して復号する第 2 の再生装置 3 3 0 0 を示している。また、図 3 4 は記録媒体 3 1 2 0 に記録される各種データの具体例を示している。

20 図 3 1 の記録装置 3 1 0 0 が図 1 の記録装置 1 0 0 と異なる点は、コンテンツ鍵生成部 3 1 0 9 で外部から入力される第 1 及び第 2 のシードを用いてコンテンツ鍵を生成し、メディア鍵を用いて第 1 及び第 2 のシードをそれぞれ第 1 のシード暗号化部 3 1 0 7 及び第 2 のシード暗号化部 3 1 0 8 で暗号化して、記録媒体 3 1 2 0 に記録するようにしたこと
25 である。その他の点は図 1 の記録装置 1 0 0 と同じであるので、その説明は省略する。

記録媒体 3 1 2 0 は、第 1 の暗号化メディア鍵データを記録する第 1 の暗号化メディア鍵データ記録領域 3 1 2 1 と、第 2 の暗号化メディア鍵データを記録する第 2 の暗号化メディア鍵データ記録領域 3 1 2 2 と、第 1 のシード暗号化部 3 1 0 7 が生成した第 1 の暗号化シードを記録する第 1 の暗号化シード記録領域 3 1 2 3 と、第 2 のシード暗号化部 3 1 0 8 が生成した第 2 の暗号化シードを記録する第 2 の暗号化シード記録領域 3 1 2 4 と、暗号化コンテンツを記録する暗号化コンテンツ記録領域 3 1 2 5 とを備える。

第 1 の再生装置 3 2 0 0 は、読み出し装置 3 2 1 0 及び復号装置 3 2 2 0 とから構成される。

読み出し装置 3 2 1 0 は、デバイス鍵を秘密に保有するデバイス鍵格納部 3 2 1 1 と、デバイス鍵を用いて記録媒体 3 1 2 0 から読み出した第 2 の暗号化メディア鍵データを復号してメディア鍵を取得する第 2 のメディア鍵復号部 3 2 1 2 と、取得したメディア鍵を用いて記録媒体から読み出した第 2 の暗号化シードを復号して第 2 のシードを取得する第 2 のシード復号部 3 2 1 3 と、取得した第 2 のシードを、記録媒体 3 2 2 0 から読み出した第 1 の暗号化メディア鍵データ、第 1 の暗号化シード、及び暗号化コンテンツとともに復号装置 3 2 2 0 に供給する。本実施の形態において、読み出し装置 3 2 1 0 は上記した構成要素がハードウェアで実装されており、第 2 のカテゴリに属するものとした。

復号装置 3 2 2 0 は、デバイス鍵を秘密に保有するデバイス鍵格納部 3 2 2 1 と、デバイス鍵を用いて読み出し装置 3 2 1 0 から供給される第 1 の暗号化メディア鍵データを復号してメディア鍵を取得する第 1 のメディア鍵復号部 3 2 2 2 と、取得したメディア鍵を用いて読み出し装置 3 2 1 0 から供給される第 1 の暗号化シードを復号して第 1 のシードを取得する第 1 のシード復号部 3 2 2 3 と、取得した第 1 のシードと読

み出し装置 3 2 1 0 から供給される第 2 のシードを用いてコンテンツ鍵を生成するコンテンツ鍵生成部 3 2 2 4 と、生成したコンテンツ鍵を用いて読み取り装置 3 2 1 0 から供給される暗号化コンテンツを復号するコンテンツ復号部 3 2 2 5 とを備える。本実施の形態 6 において、復号装置 3 2 2 0 は上記した構成要素がソフトウェアで実装されており、第 1 のカテゴリに属するものとした。尚、第 1 のシード及び第 2 のシードをそれぞれ 6 4 ビットとし、それぞれの上位 2 8 ビットを、コンテンツ鍵生成部 3 1 0 9 及び 3 2 2 4 においてビット連結して、5 6 ビットのコンテンツ鍵を得る等の方法が考えられる。

- 10 第 2 の再生装置 3 3 0 0 は、第 2 のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部 3 3 0 1 と、デバイス鍵を用いて記録媒体 3 1 2 0 から読み出した第 2 の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部 3 3 0 2 と、取得したメディア鍵を用いて記録媒体から読み出した第 1 の暗号化シードを復号して第 1 のシードを取得する第 1 のシード復号部 3 3 0 3 と、取得したメディア鍵を用いて記録媒体 3 1 2 0 から読み出した第 2 の暗号化シードを復号して第 2 のシードを取得する第 2 のシード復号部 3 3 0 4 と、取得した第 1 のシードと第 2 のシードからコンテンツ鍵を生成するコンテンツ鍵生成部 3 3 0 5 と、生成したコンテンツ鍵を用いて記録媒体 3 1 2 0 から読み出した暗号化コンテンツを復号するコンテンツ復号部 3 3 0 6 とを備える。本実施の形態 6 において、第 2 の再生装置 3 3 0 0 は上記した構成要素がハードウェアで実装されており、第 2 のカテゴリに属するものとした。

25 本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第 1 のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光

ディスクドライブのようにハードウェアで実装される装置を第2のカテゴリに属する装置とした。

図34は、 m 台の第1のカテゴリの復号装置及び n 台の第2のカテゴリの装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1の
5 カテゴリの復号装置2と第2のカテゴリの装置3が無効化されていると
した場合の、記録媒体3120に記録される各種データの具体例を示している。図34中で、第1のカテゴリの復号装置 i ($i = 1 \sim m$) が保有するデバイス鍵を DKA_i 、第2のカテゴリの装置 j ($j = 1 \sim n$) が保有するデバイス鍵を DKA_j としている。また、 $E_a(X, Y)$ 、
10 $E_b(X, Y)$ 、 $E_c(X, Y)$ 、 $E_d(X, Y)$ 、及び $E_e(X, Y)$ はデータ Y を鍵データ X を用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長56ビットのDES暗号を使用した。

第1の暗号化メディア鍵データ記録領域3121及び第2の暗号化メディア鍵データ記録領域3122に記録されるデータは、それぞれ、前記した実施の形態1における第1の暗号化メディア鍵データ記録領域121及び第2の暗号化メディア鍵データ記録領域122に記録されるデータと同じであるので、その説明は省略する。

(第1の暗号化シード記録領域3123)

20 第1の暗号化シード記録領域3123にはメディア鍵(MK)で暗号化された第1のシード(SD1)が記録されている。

(第2の暗号化シード記録領域3124)

第2の暗号化シード記録領域3124にはメディア鍵(MK)で暗号化された第2のシード(SD2)が記録されている。

25 (暗号化コンテンツ記録領域3125)

暗号化コンテンツ記録領域3125には、コンテンツ鍵(CK)で暗

号化されたコンテンツが記録されている。

以上のように構成された本発明の実施の形態において、例えば第 1 のカテゴリの復号装置に付与したデバイス鍵の多数や、第 1 の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第 1 のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

(システム更新の具体例 1)

第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 3 1 2 0 に記録する各種データの具体例 1 を図 3 5 に示す。図 3 4 との違いは、第 1 の暗号化メディア鍵データの生成に用いるデバイス鍵を $DKA_1 \sim DKA_m$ から $DKA'_1 \sim DKA'_m$ に変更したことである。これは、前記した実施の形態 1 で述べたシステム更新の具体例 1 と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵 ($DKA'_1 \sim DKA'_m$) のうちの各デバイス鍵は、システム更新前のデバイス鍵 ($DKA_1 \sim DKA_m$) のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が DKA_2 以外に存在したとしても、そのデバイス鍵を使って図 3 5 の記録媒体から読み出した第 1 の暗号化メディア鍵データを復号してメディア鍵 (MK) を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第 2 の暗号化メディア鍵データの生成に用いるデバイス鍵 ($DKB_1 \sim DKB_n$) は変更されていないので、第 2 のカテゴリに属する装置には何らの変更を加える必要がない。

(システム更新の具体例 2)

第 1 のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 3 1 2 0 に記録する各種データの具体例 2 を図 3 6 に示す。図 3 4 との違いは、第 1 の暗号化メディア鍵データの生成に用いるデバイス鍵を $DKA_1 \sim DKA_m$ から $DKA'_1 \sim DKA'_m$ に変更したことと、暗号化アルゴリズムを $E_a(X, Y)$ から $E_{a'}(X, Y)$ に変更したことである。これは、前記した実施の形態 1 で述べたシステム更新の具体例 2 と同様であるので、詳細についての説明は省略する。

10 ここで、新たなデバイス鍵 ($DKA'_1 \sim DKA'_m$) のうちの各デバイス鍵は、システム更新前のデバイス鍵 ($DKA_1 \sim DKA_m$) のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が DKA_2 以外に存在したとしても、そのデバイス鍵を使って図 3 6 の記録媒体から読み出した第 1 の暗号化
15 メディア鍵データを復号してメディア鍵 (MK) を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

20 なお、上記したシステム更新に際して、第 2 の暗号化メディア鍵データの生成に用いるデバイス鍵 ($DKB_1 \sim DKB_n$) 及び第 2 の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第 2 のカテゴリに属する装置には何らの変更を加える必要がない。

以上のように構成された本発明の実施の形態 5 によれば、第 1 のカテ
25 ゴリの装置 (復号装置 3 2 2 0) 及び第 2 のカテゴリの装置 (読み出し装置 3 2 1 0 及び第 2 の再生装置 3 3 0 0) は、それぞれ異なるカテ

りの装置を無効化するための第 1 もしくは第 2 の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第 1 の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第 2 の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第 1 のカテゴリーの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第 1 のカテゴリーの復号装置に付与するデバイス鍵の鍵長や第 1 の暗号化メディア鍵データの生成アルゴリズムを変更することで、第 2 のカテゴリーの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第 1 のカテゴリーの復号装置 3 2 2 0 には、第 2 の暗号化シードを復号するためのアルゴリズムは実装されていないので、第 1 のカテゴリーの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツ毎に異なる第 2 の暗号化シードを復号することはできず、第 1 のカテゴリーに対する不正行為がシステム全体に影響することを防ぐことができ、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第 1 のカテゴリーは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第 2 のカテゴリーは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図 3 1 で、メディア鍵、第 1 のシード、及び第 2 のシードが記録装置 3 1 0 0 の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置 3 1 0 0 がメディア鍵、第 1 のシード、及び第 2 のシードを格納する格納部を有する構成であってもよい。また、記録装置 3 1 0 0 がメディア鍵、第 1 のシード、及び

第2のシードをその都度生成する生成部を有する構成であってもよい。

また、図31では、第1のシード及び第2のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第1及び第2のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図31に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図31中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図35の $E_a(DKA'2, 0)$ や図36の $E_{a'}(DKA'2, 0)$ のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いるこ

とができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第 1 の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第 1 のカテゴリに属する復号装置の台数を増やすことが可能となる。

また、本実施の形態では、図 3 4 に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献 1 として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長 56 bit の DES、あるいはシステム更新後の暗号アルゴリズムとして鍵長 112 bit の 2 キートリプル DES を用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長 128 bit の AES 等を用いても良い。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態 2 のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

(実施の形態 7)

本発明の実施の形態 7 は、実施の形態 6 のシステムにおいて、第 1 のカテゴリと第 2 のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第 1 の暗号化シードの階層を設けるようにしたものである。

以下、本発明の実施の形態 7 について、図面を参照にしながら説明する。図 37 は、コンテンツを暗号化して記録する記録装置 3700 及び記録媒体 3720 を示しており、図 38 は、記録媒体 3720 から暗号化コンテンツを読み出して復号する第 1 の再生装置 3800 を示しており、図 39 は、記録媒体 3720 から暗号化コンテンツを読み出して復号する第 2 の再生装置 3900 を示している。また、図 40 は記録媒体 3720 に記録される各種データの具体例を示している。

図 37 の記録装置 3700 が図 31 の記録装置 3100 と異なる点は、第 1 のカテゴリに対しては第 1 のメディア鍵を、第 2 のカテゴリに対しては第 2 のメディア鍵を、個別に設け、第 1 及び第 2 のメディア鍵をそれぞれ第 1 のメディア鍵暗号化部 3705 及び第 2 のメディア鍵暗号化部 3706 で暗号化し、第 1 のシードを第 1 及び第 2 のメディア鍵を用いてそれぞれ第 1 シード暗号化部 (1) 3707 及び第 1 のシード暗号化部 (2) 3711 で暗号化し、記録媒体 3720 に記録するようにしたことである。その他の点については、前記した実施の形態 6 の記録装置 3100 と同じであるので、その説明は省略する。

記録媒体 3720 は、第 1 の暗号化メディア鍵データを記録する第 1 の暗号化メディア鍵データ記録領域 3721 と、第 2 の暗号化メディア鍵データを記録する第 2 の暗号化メディア鍵データ記録領域 3722 と、第 1 のシード暗号化部 (1) 3707 が生成した第 1 の暗号化シード (1) を記録する第 1 の暗号化シード (1) 記録領域 3723 と、第 1 のシード暗号化部 (2) 3711 が生成した第 1 の暗号化シード (2) を記録する第 1 の暗号化シード (2) 記録領域 3726 と、第 2 の暗号化シードを記録する第 2 の暗号化シードデータ記録領域 3724 と、暗号化コンテンツを記録する暗号化コンテンツ記録領域 3725 とを備える。尚、第 2 の暗号化シードデータは、第 1 の再生装置 3800 の読み出し装置

3810及び第2の再生装置3900において第2メディア鍵を用いて復号される。

第1の再生装置3800において復号装置3820は、読み出し装置3810が記録媒体3720から読み出した第1の暗号化シード(1)を復号して第1のシードを取得する。その他の点については、前記した実施の形態6における第1の再生装置3200と同様であるので、その説明は省略する。

第2の再生装置3900は、記録媒体3720から読み出した第1の暗号化シード(2)を復号して第1のシードを取得する。その他の点については、前記した実施の形態6における第2の再生装置3300と同様であるので、その説明は省略する。

図40は、記録媒体3720に記録される各種データの具体例を示している。第1の暗号化メディア鍵データ記録領域3721には、第1のカテゴリの復号装置が保有するデバイス鍵(DKA1~DKAm)で暗号化された第1のメディア鍵(MK1)が記録されており、第2の暗号化メディア鍵データ記録領域3722には、第2のカテゴリの装置が保有するデバイス鍵(DKB1~DKBm)で暗号化された第2のメディア鍵(MK2)が記録されている。また、第1の暗号化シードデータ(1)記録領域3723には、第1のメディア鍵(MK1)で暗号化された第1のシード(SD1)が記録されており、第1の暗号化シードデータ(2)記録領域3726には、第2のメディア鍵(MK2)で暗号化された第1のシード(SD1)が記録されている。その他の点については、前記した図34と同じであるので、説明を省略する。なお、図40中の、 $E_f(X, Y)$ はデータYを鍵データXを用いて暗号化する関数を意味し、本実施の形態では鍵長56ビットのDES暗号を使用した。

以上のように構成された本発明の実施の形態7において、例えば第1

のカテゴリの復号装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの復号装置の無効化システムを更新する
5 ことになる。以下、その具体例を説明する。

(システム更新の具体例1)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体3720に記録する各種データの具体例1を図41に示す。図40との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKA_mからDKA'1~DKA'_mに変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例1と同様であるので、詳細についての説明は省略する。
10

(システム更新の具体例2)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体3720に記録する各種データの具体例2を図42に示す。図40との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKA_mからDKA'1~DKA'_mに変更したこと、暗号化アルゴリズムをE_a(X, Y)からE_{a'}(X, Y)に変更したこと、及び第1の暗号化シード(1)の暗号化アルゴリズムをE_c(X, Y)からE_{c'}(X, Y)に変更したことである。これは、前記した実施の形態3で述べたシステム更新の具体例2と同様であるので、詳細についての説明は省略する。
15
20

以上のように構成された本発明の実施の形態7によれば、前記した実施の形態6同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第1のカテゴリと第2のカテゴリに対して個別にメデ
25

ィア鍵を設け、それぞれを用いた暗号化シードの階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第１のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図３７で、第１のメディア鍵、第２のメディア鍵、第１のシード、及び第２のシードが記録装置３７００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置３７００がこれらを格納する格納部を有する構成であってもよい。また、記録装置３７００がこれらをその都度生成する生成部を有する構成であってもよい。

また、図３７では、第１のシード及び第２のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第１及び第２のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図３７に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリの

デバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図 3 7 中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第 1 の暗号化メディア鍵データを生成する際に、図 4 1 の $E_a(DKA', 2, 0)$ や図 4 2 の $E_{a'}(DKA', 2, 0)$ のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第 1 の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第 1 のカテゴリに属する復号装置の台数を増やすことが可能となる。

また、本実施の形態では、図 4 0 に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献 1 として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長 56 bit の DES、あるいはシステム更新後の暗号アルゴリズムとして鍵長 112

b i t の 2 キートリプル D E S を用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長 1 2 8 b i t の A E S 等を用いても良い。

5 なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はこれに限定されるものではない。前記した実施の形態 2 のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コン
10 テンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

15 本発明によれば、第 1 のカテゴリの装置及び第 2 のカテゴリの装置は、それぞれ異なるカテゴリの装置を無効化するための第 1 もしくは第 2 の暗号化メディア鍵を読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。

20 また、第 1 の暗号化メディア鍵の生成に用いる暗号化アルゴリズムを第 2 の暗号化メディア鍵の生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第 1 のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第 1 のカテゴリの再生装置に付与するデバイス鍵の鍵長や第 1 の暗号化メディア鍵の生成アルゴリズムを変更することで、第 2 のカテゴリの再生装置に影響を与えることなく、無効化システムを更新することができる。

産業上の利用の可能性

25 本発明にかかる著作権保護システムは、装置内に設けるメモリのサイズを小さくでき、かつ、あるカテゴリの装置が不正に解析されてアルゴ

リズムや多数の鍵が暴露された場合にも、そのカテゴリの装置用の暗号化・復号のアルゴリズムや鍵長を変更することで、他のカテゴリの装置に何らの変更を加えることなく、システム全体の無効化機能を維持できるという効果があり、著作物をデジタル化したコンテンツを光ディスク等5 等の大容量記録媒体に記録もしくは再生するシステムにおいて、復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される記録装置もしくは再生装置と、堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される記録装置もしくは再生装置とが存在するような場合に有用である。

請 求 の 範 囲

1. コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、

前記記録装置は、メディア鍵と前記N個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記N個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、

前記再生装置は、前記記録媒体から前記N個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする著作権保護システム。

2. 前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、

前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得

し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項 1 記載の著作権保護システム。

- 5 3. 前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、
前記暗号化鍵に基づいて前記コンテンツを暗号化し、

前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号する

- 10 ことを特徴とする請求項 2 記載の著作権保護システム。

4. 前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、

- 15 前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する

ことを特徴とする請求項 2 記載の著作権保護システム。

20

5. 前記 N 個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

- 前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記 N 個のメディア鍵で暗号化して N 個の暗号化コンテンツ鍵を生成し、少なくとも前記 N 個の暗号化メディア鍵データと前記 N
- 25

個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、

前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する

ことを特徴とする請求項 1 記載の著作権保護システム。

10

6. 前記再生装置は、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第 2 のカテゴリに属する第 2 再生装置、及び、前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第 2 のカテゴリの読み出し装置と前記第 2 のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第 1 のカテゴリの復号装置とを備える第 1 再生装置から構成され、

15

前記記録装置は、メディア鍵と前記第 1 のカテゴリの復号装置が保有するデバイス鍵データとから前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データを生成し、前記メディア鍵と前記第 2 のカテゴリの装置が保有するデバイス鍵データとから前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第 1 の無効化データ、前記第 2 の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、

20

25

前記第 2 再生装置は、前記記録媒体から前記第 2 の無効化データ及び

前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づいて
前記暗号化コンテンツを復号し、

前記第 1 再生装置において、前記第 2 のカテゴリの読み出し装置は、
前記記録媒体から前記第 1 の無効化データ、前記第 2 の無効化データ及
5 び前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づい
て前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記
第 1 の無効化データを前記第 1 カテゴリの復号装置に供給し、前記第 1
のカテゴリの復号装置は、前記第 2 のカテゴリの読み出し装置から供給
される前記中間データに前記第 1 の無効化データに基づいて復号処理を
10 施し前記コンテンツを取得する

ことを特徴とする請求項 1 記載の著作権保護システム。

7. コンテンツを暗号化して記録する記録装置であって、

前記記録装置は、メディア鍵と N 個 (N は 2 以上の自然数) のカテゴ
15 リに分類された各カテゴリに属する再生装置が保有するデバイス鍵デー
タとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効
化するための無効化データを前記 N 個の各カテゴリに対してそれぞれ生
成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コ
ンテンツを生成し、少なくとも前記 N 個の無効化データと前記暗号化コ
20 ンテンツを前記記録媒体に記録する

ことを特徴とする記録装置。

8. 前記 N 個の各無効化データは対応するカテゴリの再生装置が保有
するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵
25 データである

ことを特徴とする請求項 7 記載の記録装置。

9. 前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする請求項 8 記載の記録装置。

5

10. 前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする請求項 8 記載の記録装置。

10

11. 前記 N 個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記 N 個のメディア鍵で暗号化して N 個の暗号化コンテンツ鍵データを生成し、少なくとも前記 N 個の暗号化メディア鍵データと前記 N 個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録する

15

ことを特徴とする請求項 7 記載の記録装置。

20

12. 前記記録装置は、メディア鍵と第 1 のカテゴリの復号装置が保有するデバイス鍵データとから前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データを生成し、前記メディア鍵と前記第 2 のカテゴリの装置が保有するデバイス鍵データとから前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データを生成し、前記メディア鍵に基づいて

25

前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第 1 の無効化データ、前記第 2 の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録する

ことを特徴とする請求項 7 記載の記録装置。

5

13. 暗号化コンテンツが記録される記録媒体であって、

前記記録媒体には、少なくとも、メディア鍵と N 個（N は 2 以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツが記録される

ことを特徴とする記録媒体。

15 14. 前記 N 個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データである

ことを特徴とする請求項 13 記載の記録媒体。

20 15. 前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものである

ことを特徴とする請求項 14 記載の記録媒体。

25 16. 前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録される

ことを特徴とする請求項 1 4 記載の記録媒体。

- 5 1 7 . 前記 N 個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

- 10 前記記録媒体には、前記コンテンツ鍵を前記 N 個のメディア鍵で暗号化して生成された N 個の暗号化コンテンツ鍵が記録される

ことを特徴とする請求項 1 3 記載の記録媒体。

- 15 1 8 . 前記記録媒体には、少なくともメディア鍵と第 1 のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データと、前記メディア鍵と第 2 のカテゴリの装置が保有するデバイス鍵データとから生成された前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとが記録される

ことを特徴とする請求項 1 3 記載の記録媒体。

- 25 1 9 . 記録媒体に記録された暗号化コンテンツを再生する再生装置であって、

前記再生装置は N 個（N は 2 以上の自然数）のカテゴリに分類されて

おり、

前記記録媒体には、少なくともメディア鍵と前記N個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、

前記再生装置は、前記記録媒体から前記N個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする再生装置。

20. 前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、

前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項19記載の再生装置。

21. 前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、

前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項 20 記載の再生装置。

22. 前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

5 前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、

前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する
10

ことを特徴とする請求項 20 記載の再生装置。

23. 前記 N 個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、
15

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記コンテンツ鍵を前記 N 個のメディア鍵で暗号化して生成された N 個の暗号化コンテンツ鍵が記録されており、

20 前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コンテンツ鍵を
25 復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する、

ことを特徴とする請求項 19 記載の再生装置。

24. 前記記録媒体には、少なくともメディア鍵と第 1 のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データと、前記メディア鍵と第 2 のカテゴリの装置が保有するデバイス鍵データとから生成された前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記再生装置は、前記第 2 のカテゴリに属し、前記記録媒体から前記第 2 の無効化データ及び前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項 19 記載の再生装置。

25. 記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、

前記記録媒体には、少なくともメディア鍵と第 1 のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データと、前記メディア鍵と第 2 のカテゴリの装置が保有するデバイス鍵データとから生成された前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記読み出し装置は、前記第 2 のカテゴリに属し、前記記録媒体から

前記第 1 の無効化データ、前記第 2 の無効化データ及び前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第 1 の無効化データを出力する

5 ことを特徴とする読み出し装置。

26. 記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、

前記記録媒体には、少なくともメディア鍵と第 1 のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第 1 のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第 1 の無効化データと、前記メディア鍵と第 2 のカテゴリの装置が保有するデバイス鍵データとから生成された前記第 2 のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第 2 の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記第 2 のカテゴリの読み出し装置は、前記記録媒体から前記第 1 の無効化データ、前記第 2 の無効化データ及び前記暗号化コンテンツを読み出し、前記第 2 の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第 1 の無効化データを出力し、

前記復号装置は、前記第 1 のカテゴリに属し、前記第 2 のカテゴリの読み出し装置から供給される前記中間データに前記第 1 の無効化データに基づいて復号処理を施して前記コンテンツを取得する

25 ことを特徴とする復号装置。

27. 記録媒体に記録された暗号化コンテンツを再生する再生装置であって、請求項25記載の読み取り装置と請求項26記載の復号装置とから構成される

ことを特徴とする再生装置。

5

28. コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

10

前記記録装置及び前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、

15

前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記N個の各カテゴリに対してそれぞれ生成し、生成した前記N個の無効化データを前記記録媒体に記録し、

20

前記記録装置は、前記記録媒体から前記N個の無効化データのうち、前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、

25

前記再生装置は、前記記録媒体から前記N個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする著作権保護システム。

29. メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記N個の各カテゴリに対してそれぞれ生成し、生成した前記N個の無効化データを前記記録媒体に記録する

ことを特徴とする鍵生成装置。

10 30. コンテンツを暗号化して記録する記録装置であって、

メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録媒体から、前記N個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、

読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、

生成した前記暗号化コンテンツを前記記録媒体に記録する

20 ことを特徴とする記録装置。

31. コンテンツを暗号化して記録する記録装置に用いる記録方法であって、

メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効

化データを前記N個の各カテゴリに対してそれぞれ生成する生成ステップと、

前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、

- 5 少なくとも前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含む
ことを特徴とする記録方法。

32. 記録媒体に記録された暗号化コンテンツを再生する再生装置に
10 用いる再生方法であって、

前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、

- 前記記録媒体には、少なくともメディア鍵と前記N個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリ
15 の特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、

前記再生方法は、

- 前記記録媒体から前記N個の無効化データのうち前記再生装置が属する
20 カテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、

前記読み出しステップにおいて読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する復号ステップとを含む

ことを特徴とする再生方法。

25

33. コンテンツを暗号化して記録する記録装置に用いるプログラム

であって、

メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各
カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カ
テゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効
5 化データを前記N個の各カテゴリに対してそれぞれ生成する生成ステッ
プと、

前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテ
ンツを生成する暗号化コンテンツ生成ステップと、

少なくとも前記N個の無効化データと前記暗号化コンテンツを前記記
10 録媒体に記録する記録ステップとを含む
ことを特徴とするプログラム。

34. 記録媒体に記録された暗号化コンテンツを再生する再生装置に
用いるプログラムであって、

15 前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されて
おり、

前記記録媒体には、少なくともメディア鍵と前記N個の各カテゴリの
再生装置が保有するデバイス鍵データとから生成された前記各カテゴリ
の特定の再生装置が保有するデバイス鍵を無効化するための無効化デー
20 タと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗
号化コンテンツとが記録されており、

前記プログラムは、

前記記録媒体から前記N個の無効化データのうち前記再生装置が属す
るカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み
25 出しステップと、

前記読み出しステップにおいて読み出した前記無効化データに基づい

て前記暗号化コンテンツを復号する復号ステップとを含む
ことを特徴とするプログラム。

図1

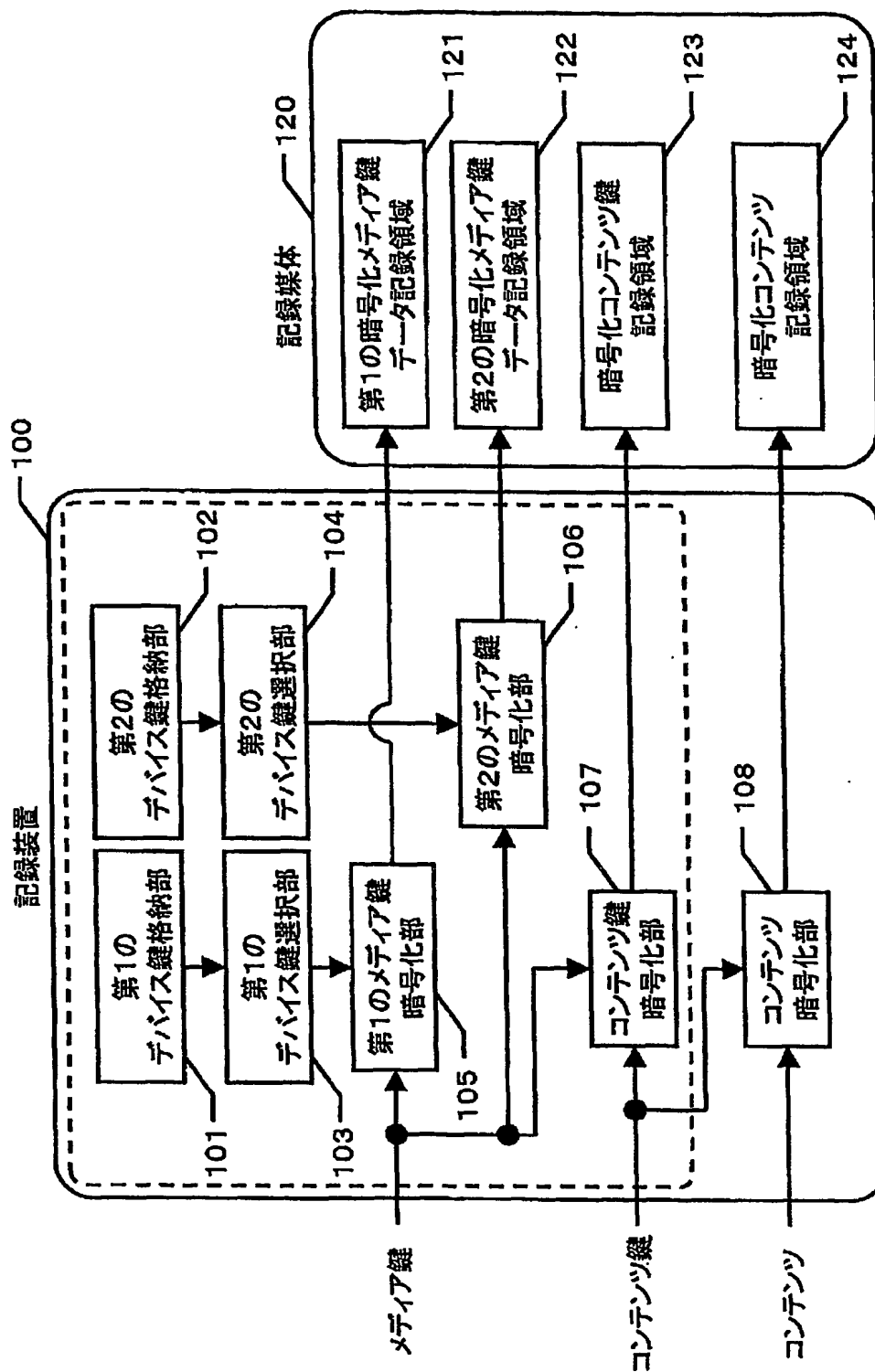


図2

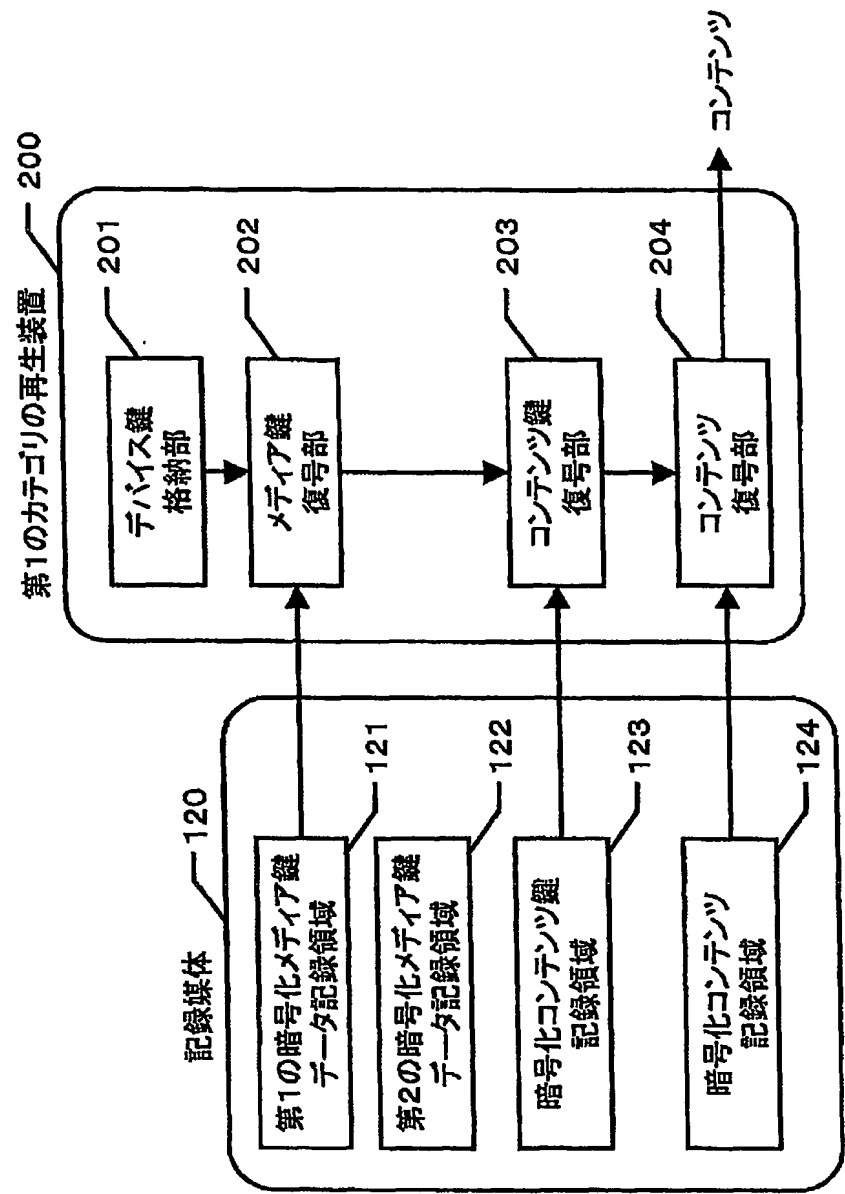


図3

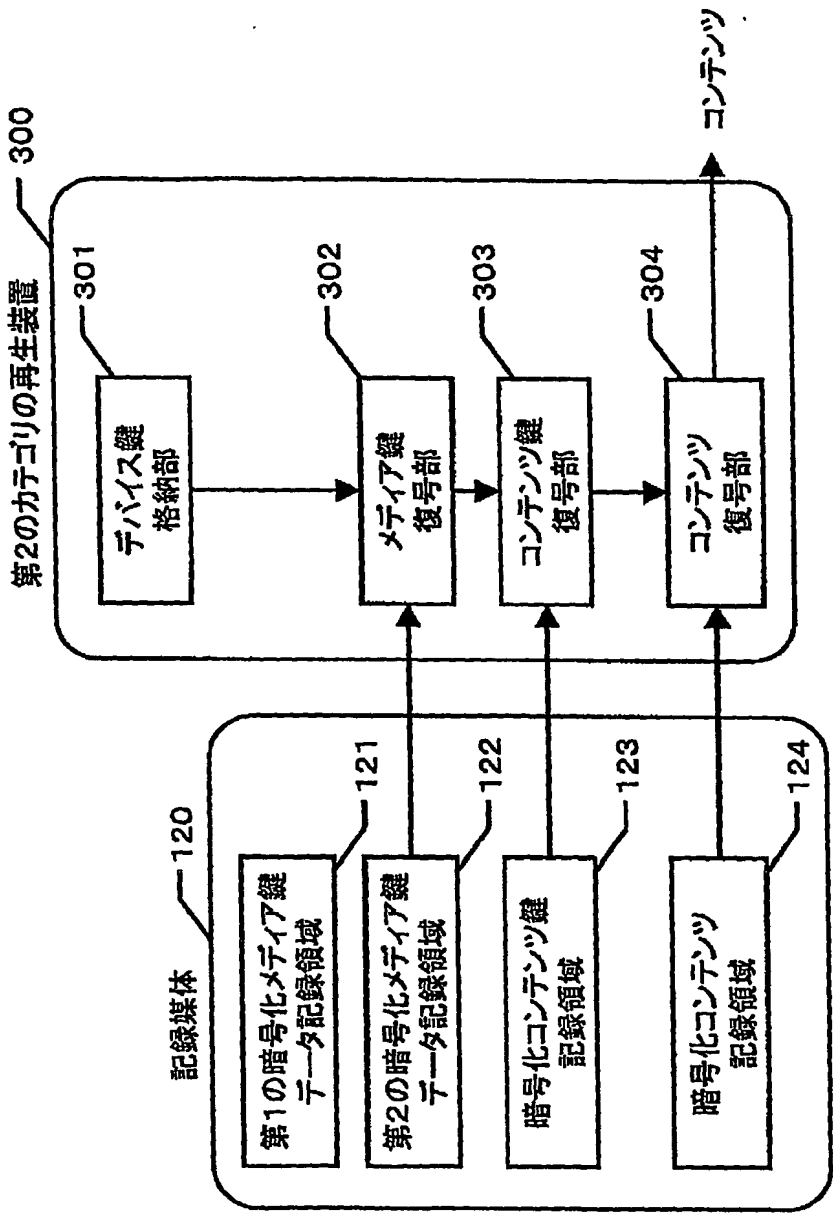


図4

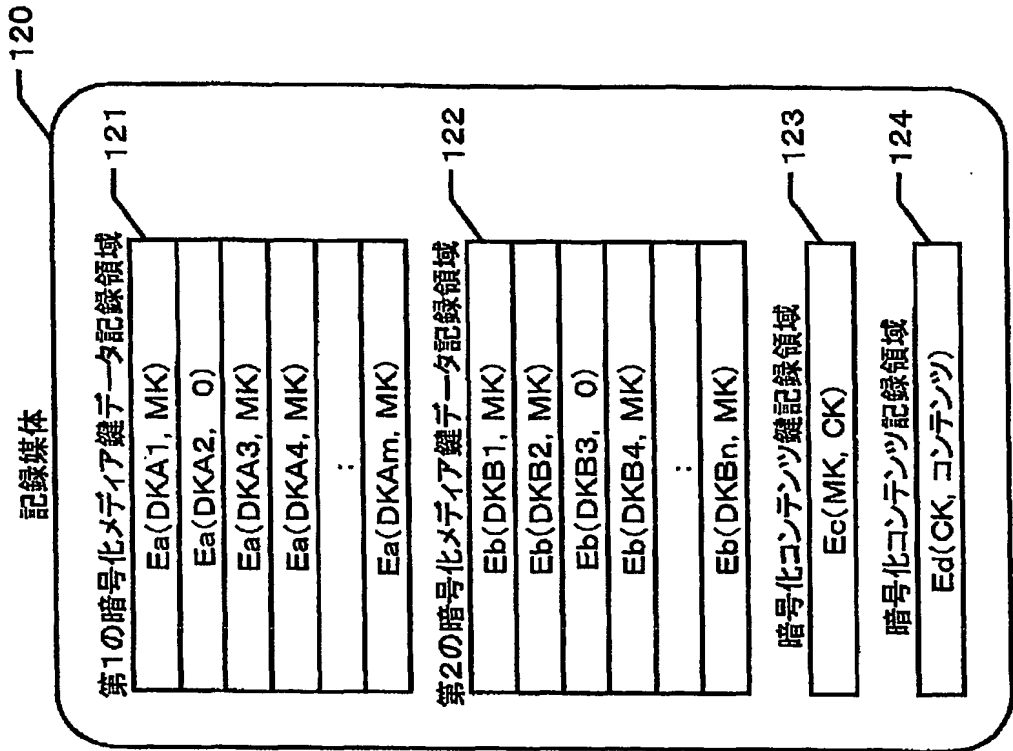


図5

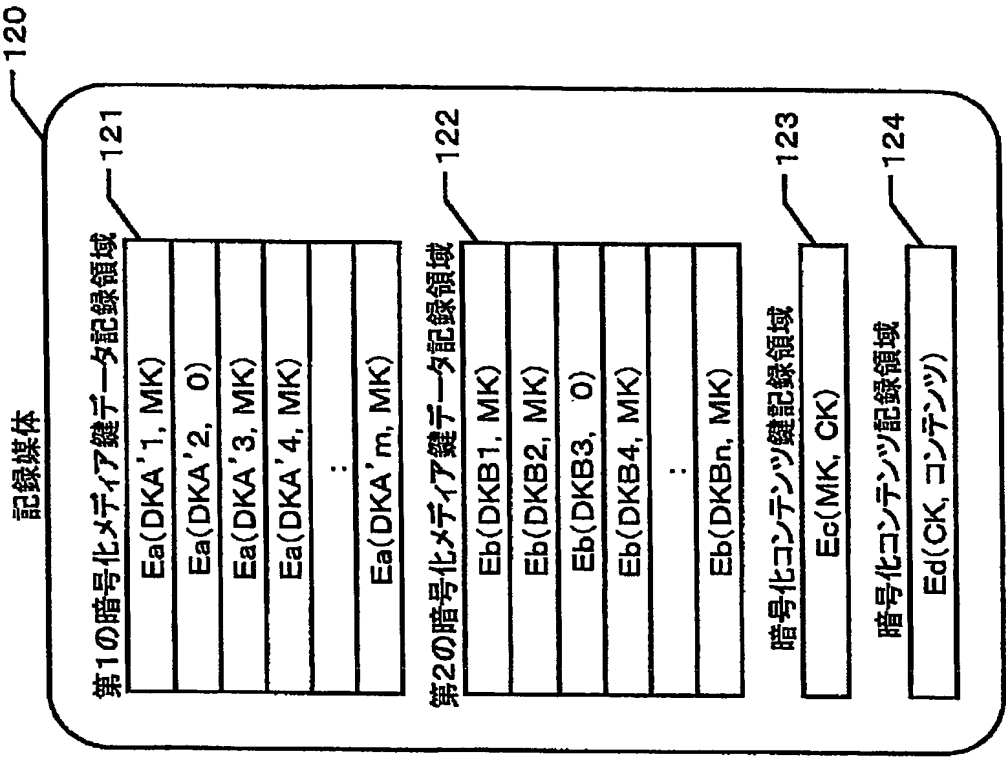


図6

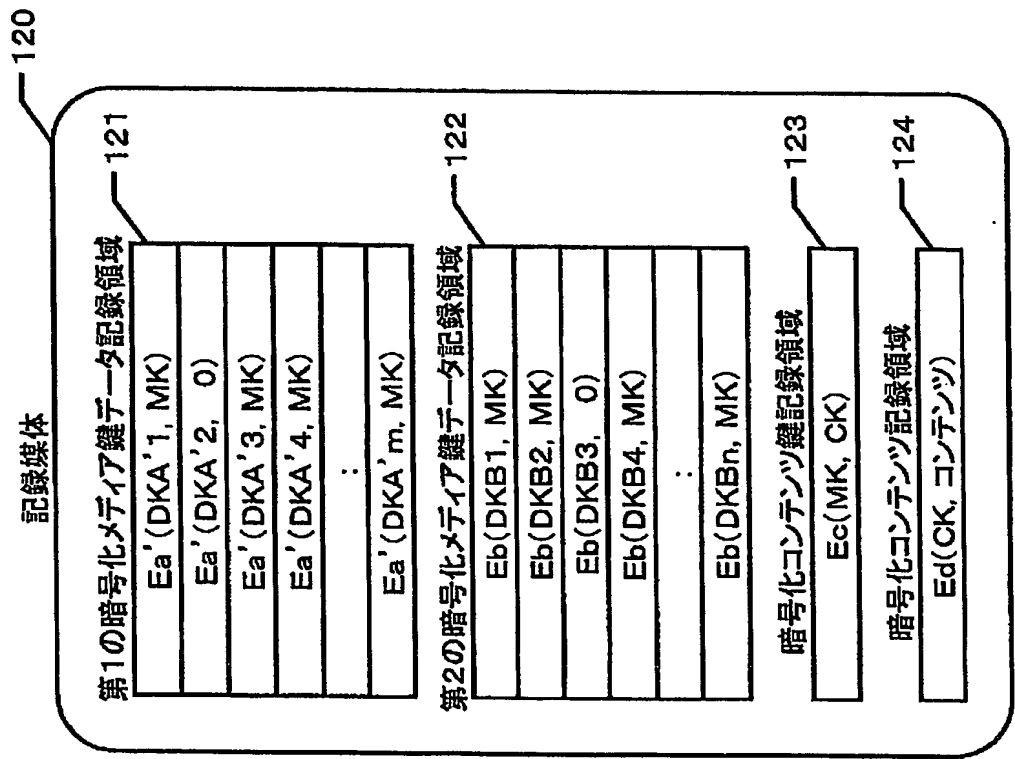


図7

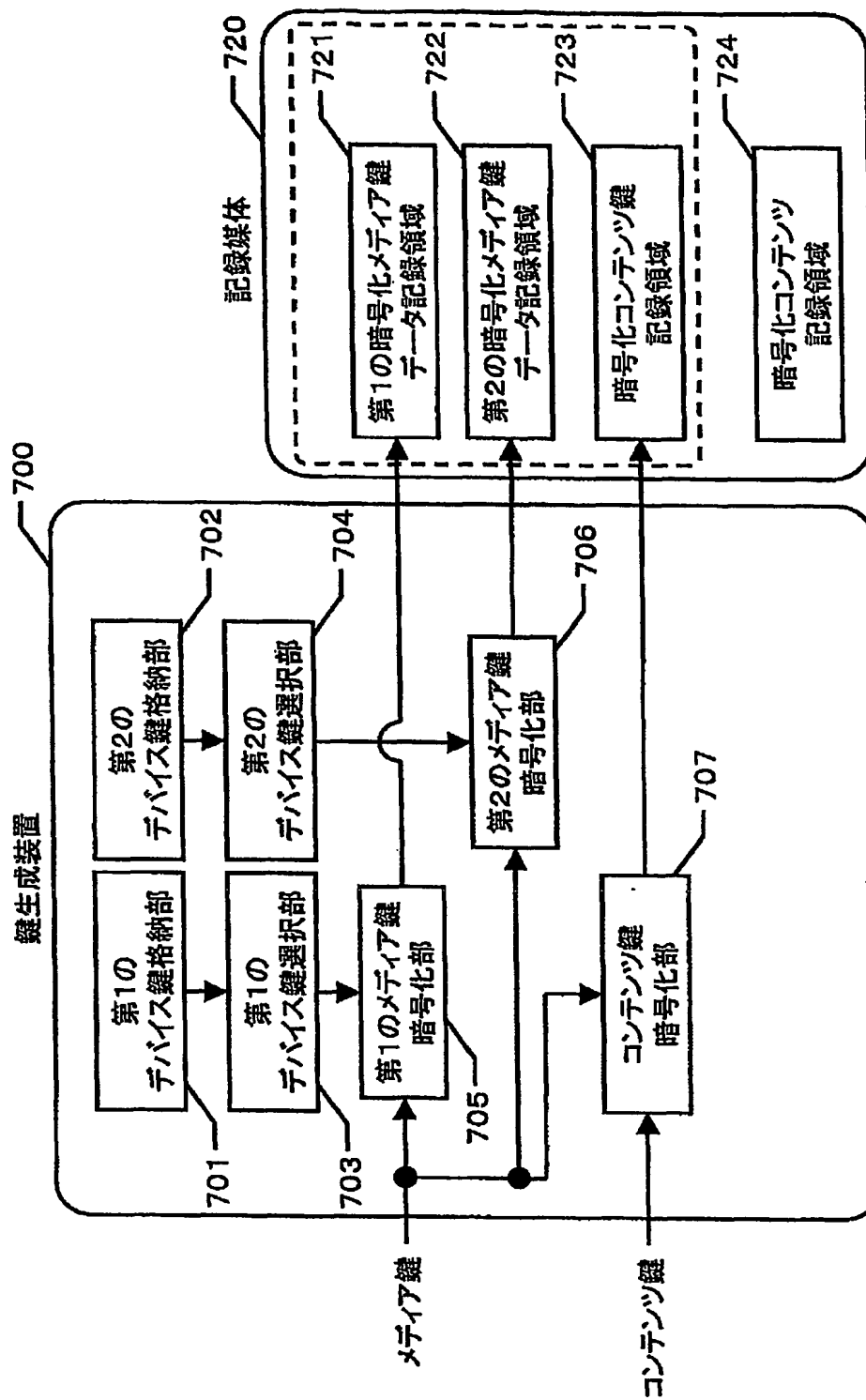


図8

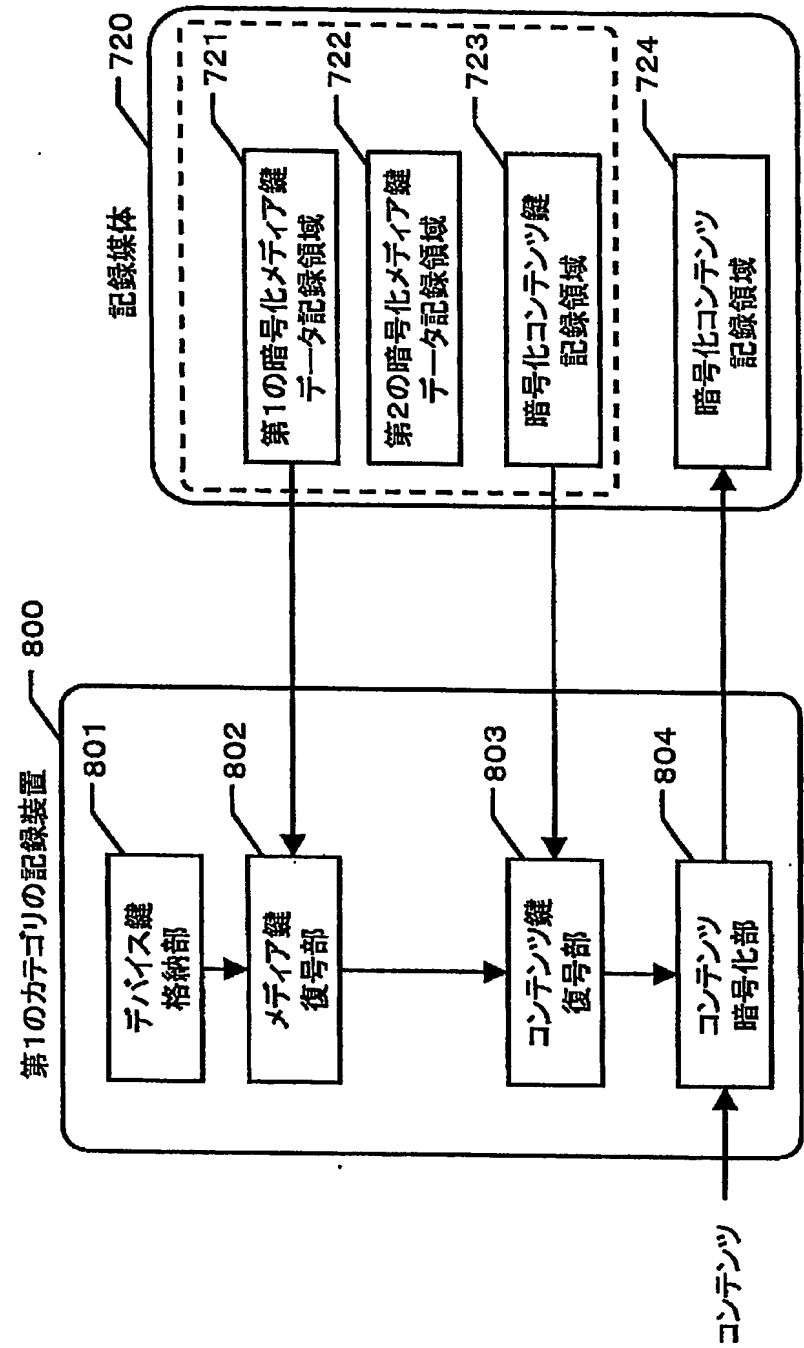


図9

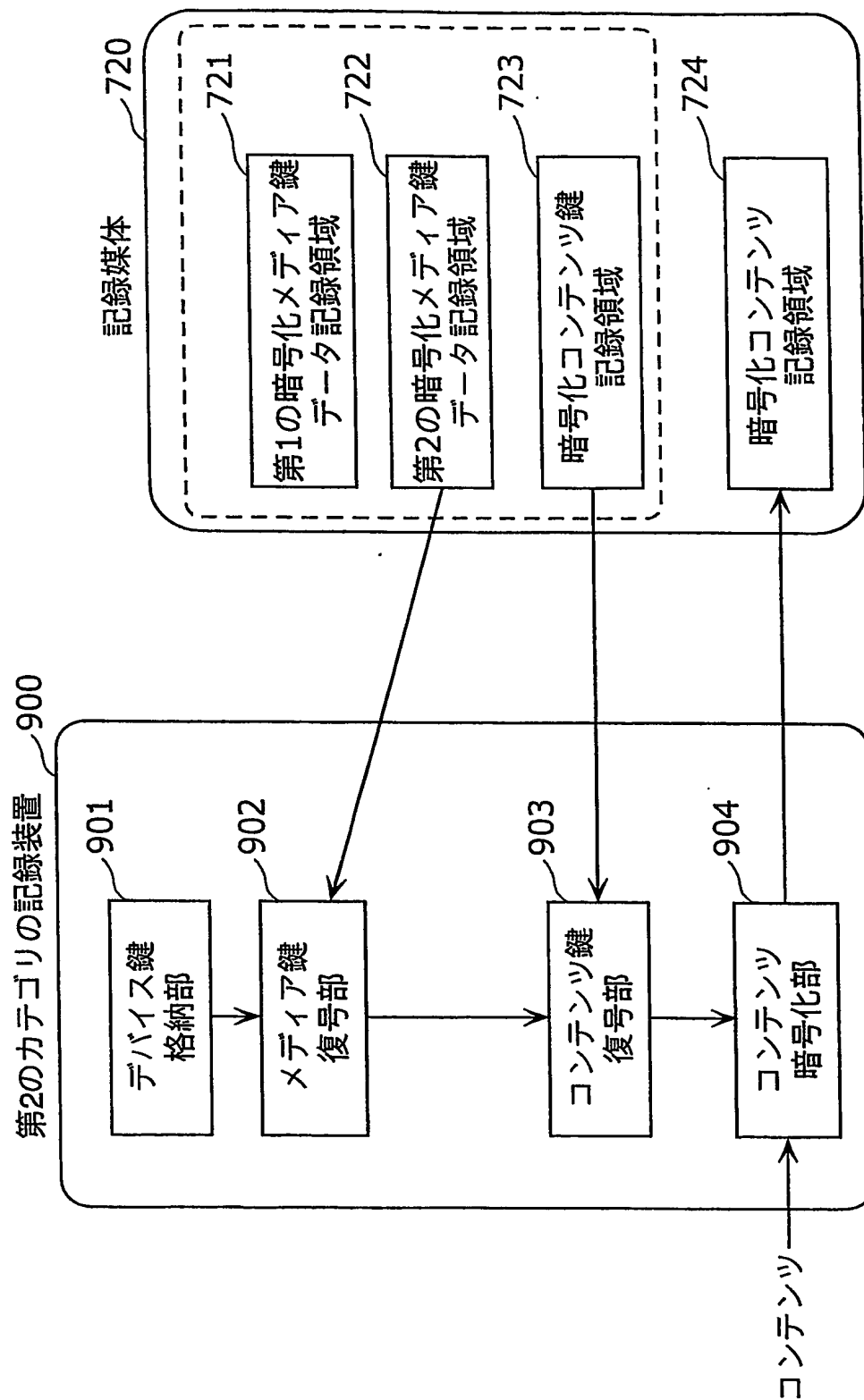


図10

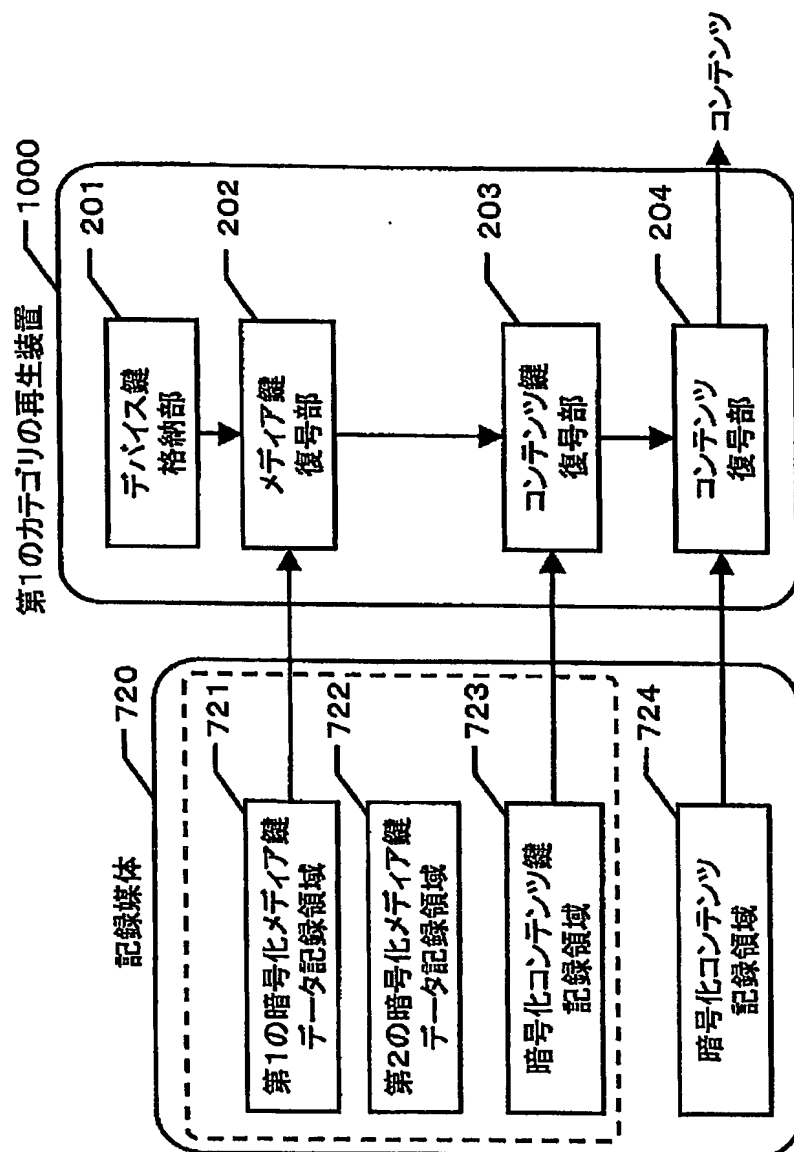


図11

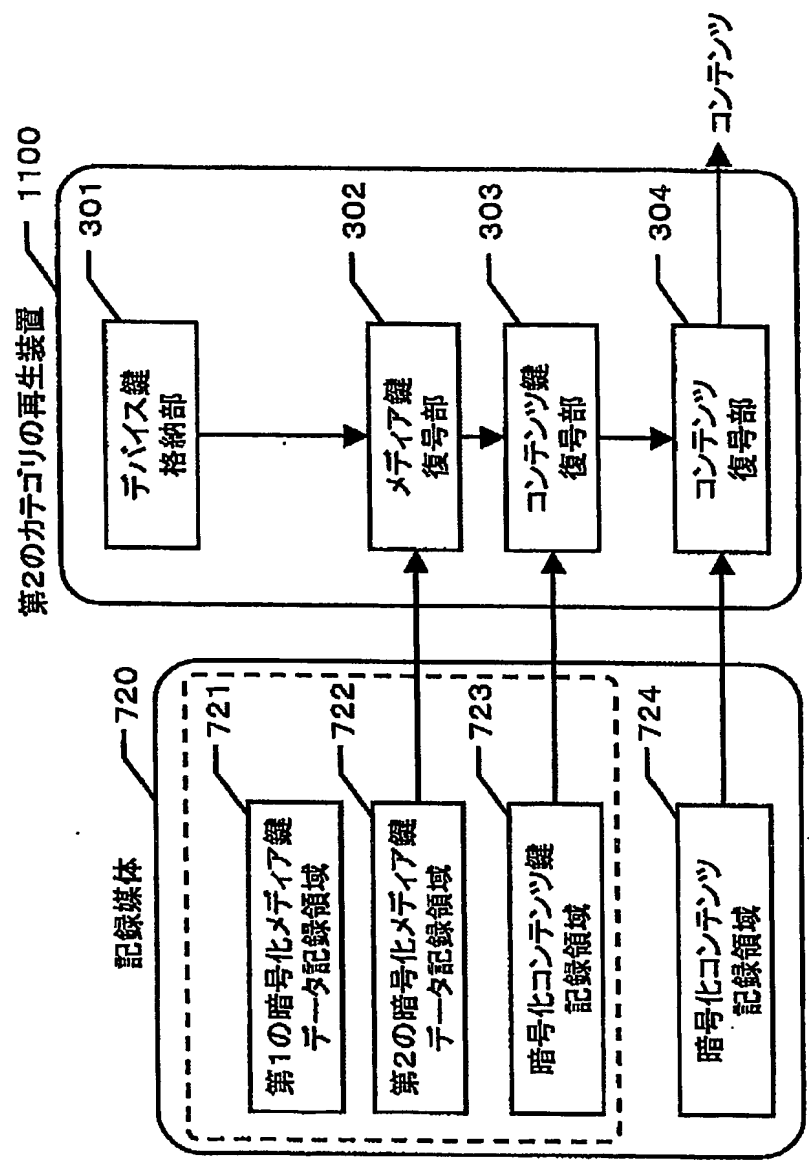


図12

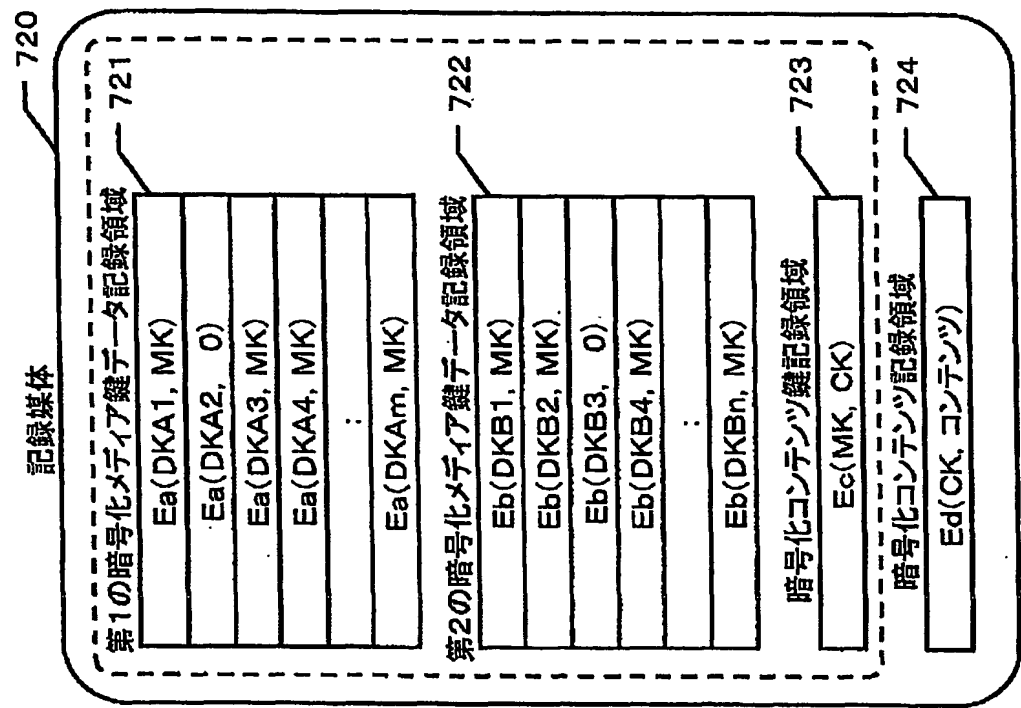


図13

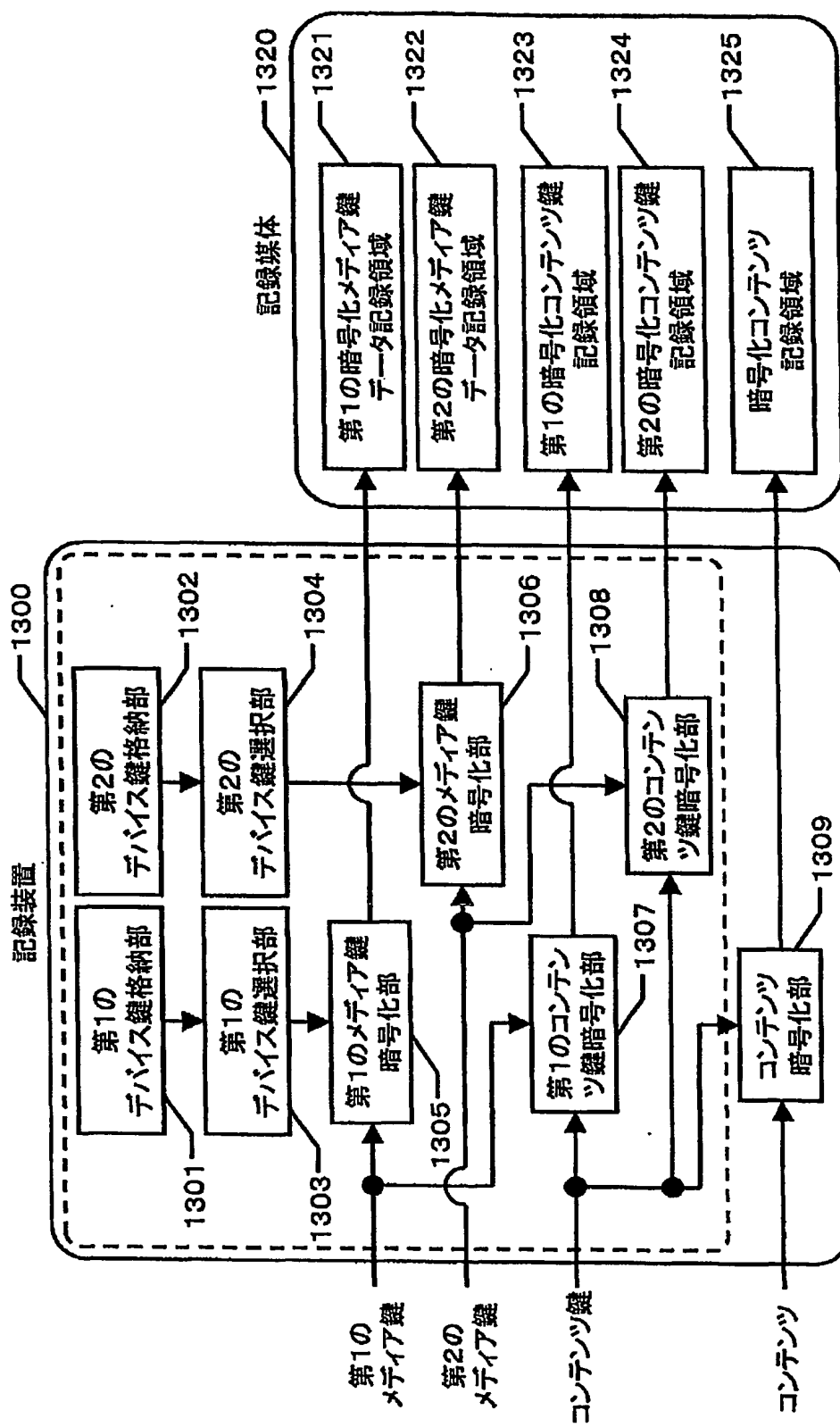


図14

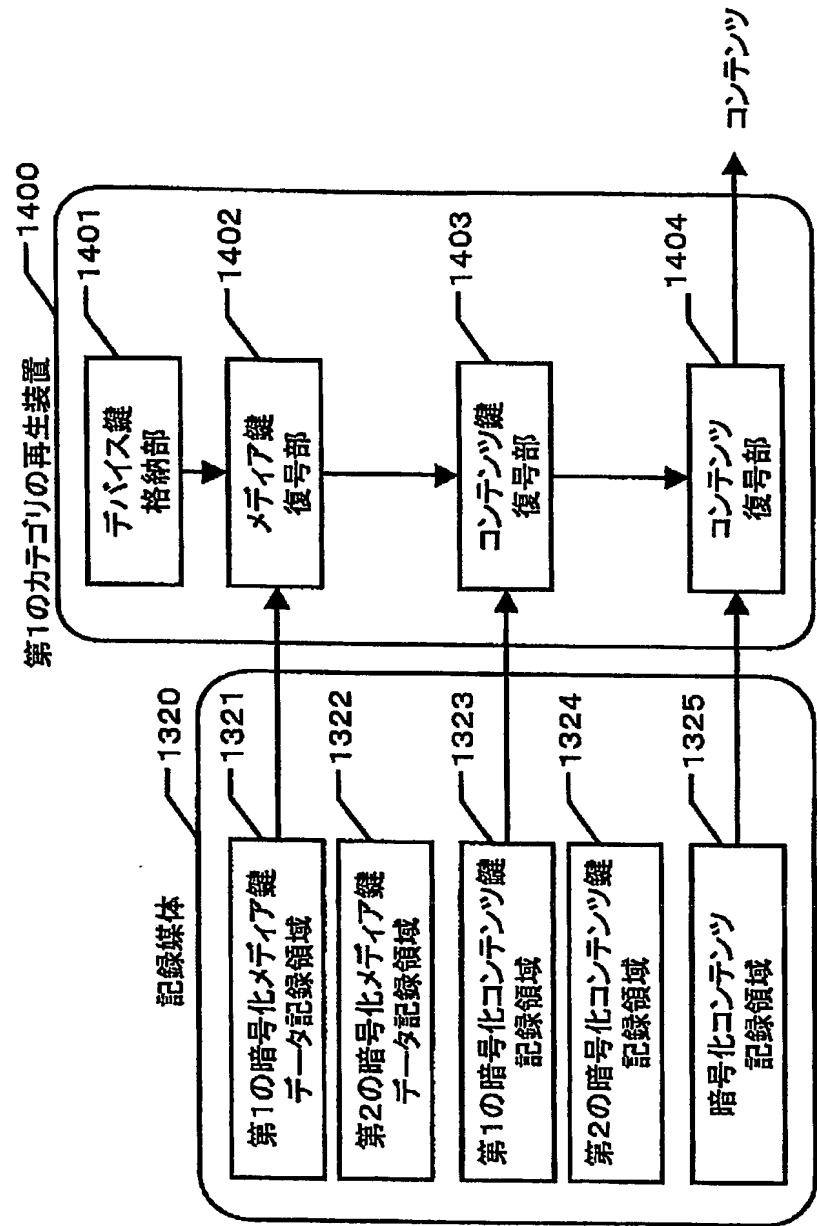


図15

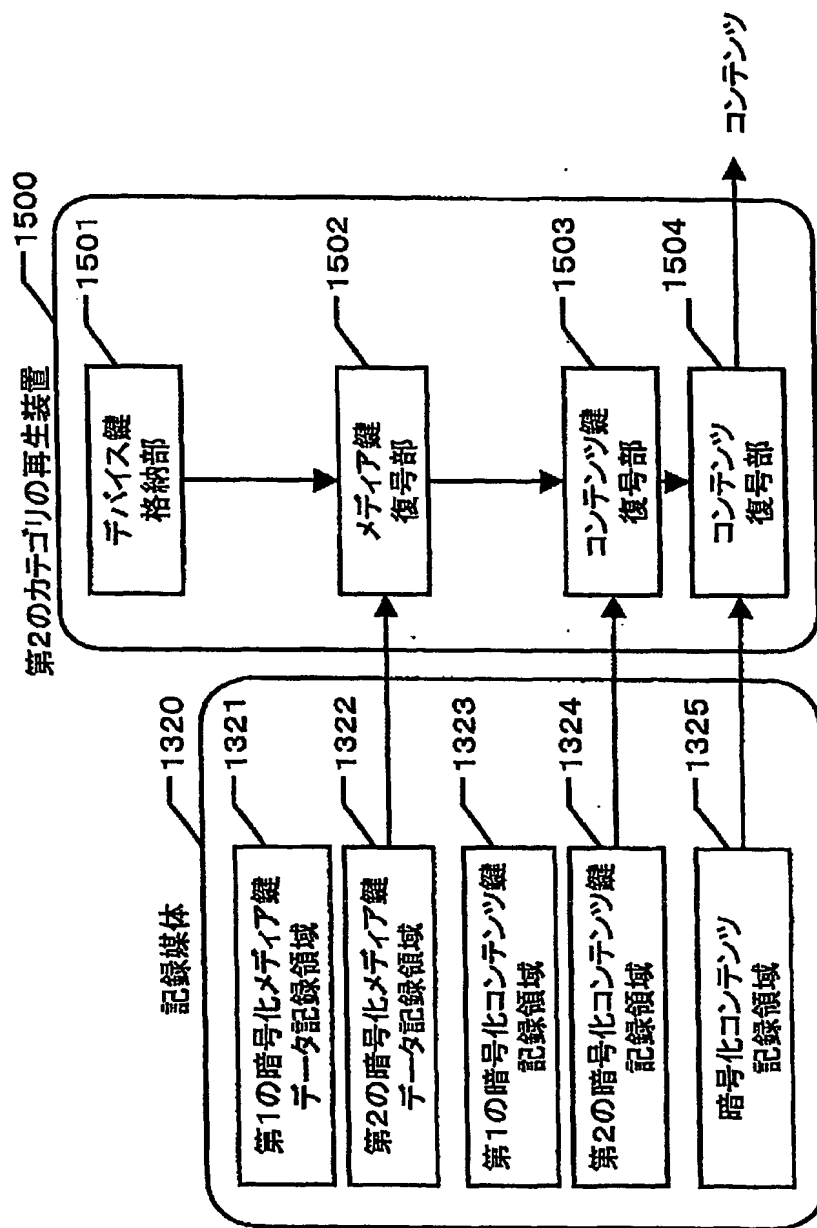


図16

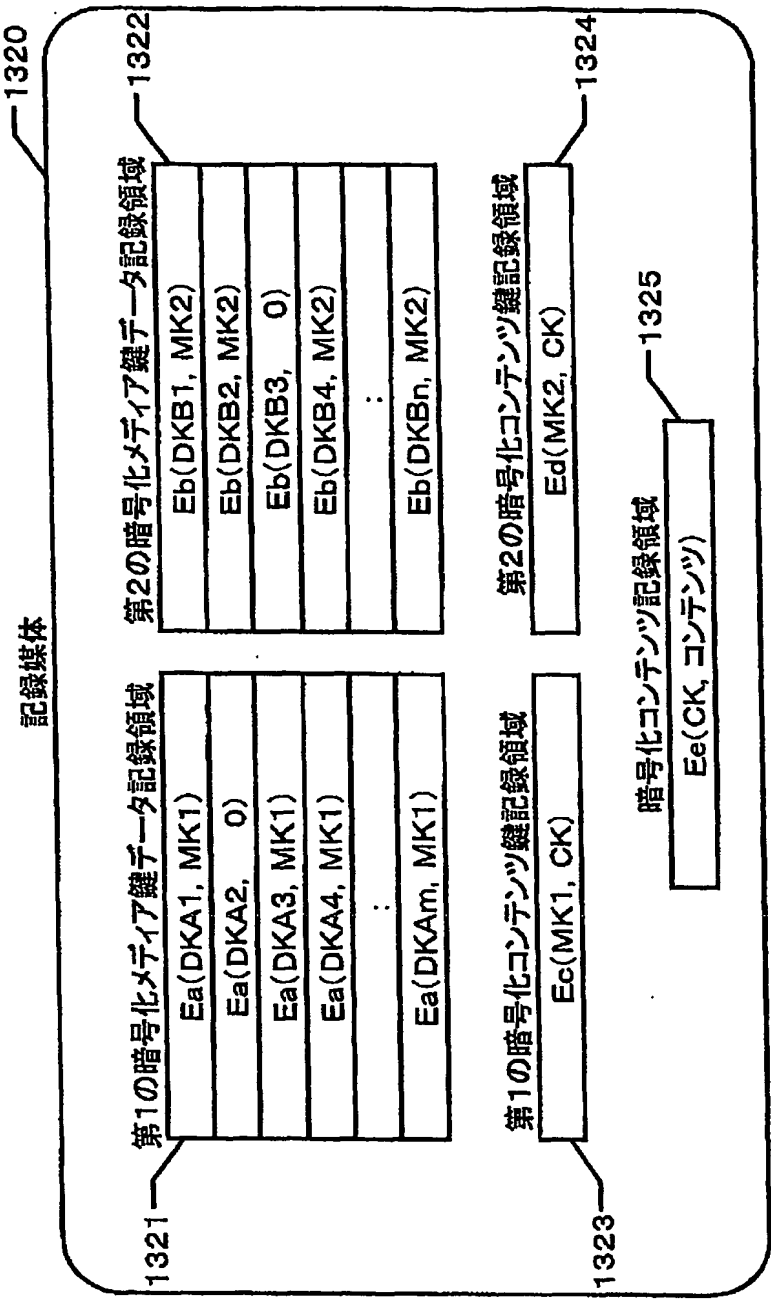


図17

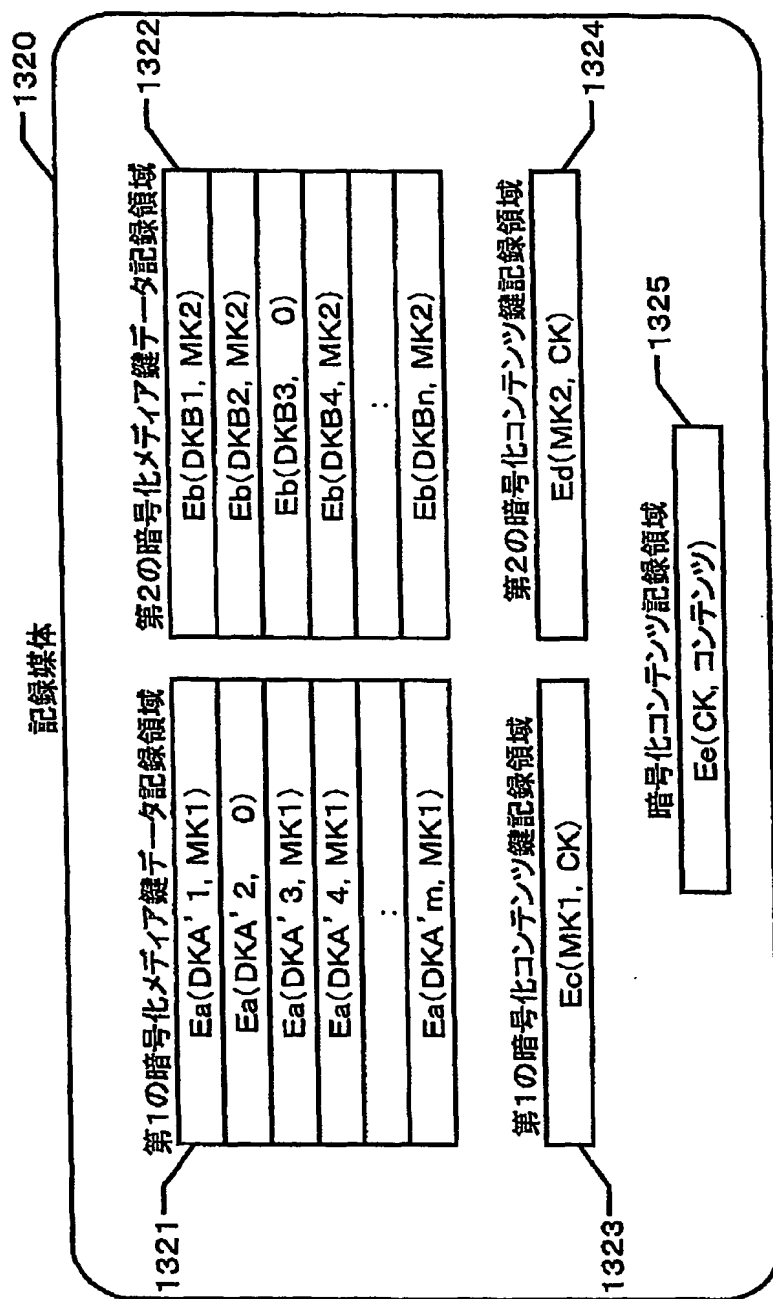


図18

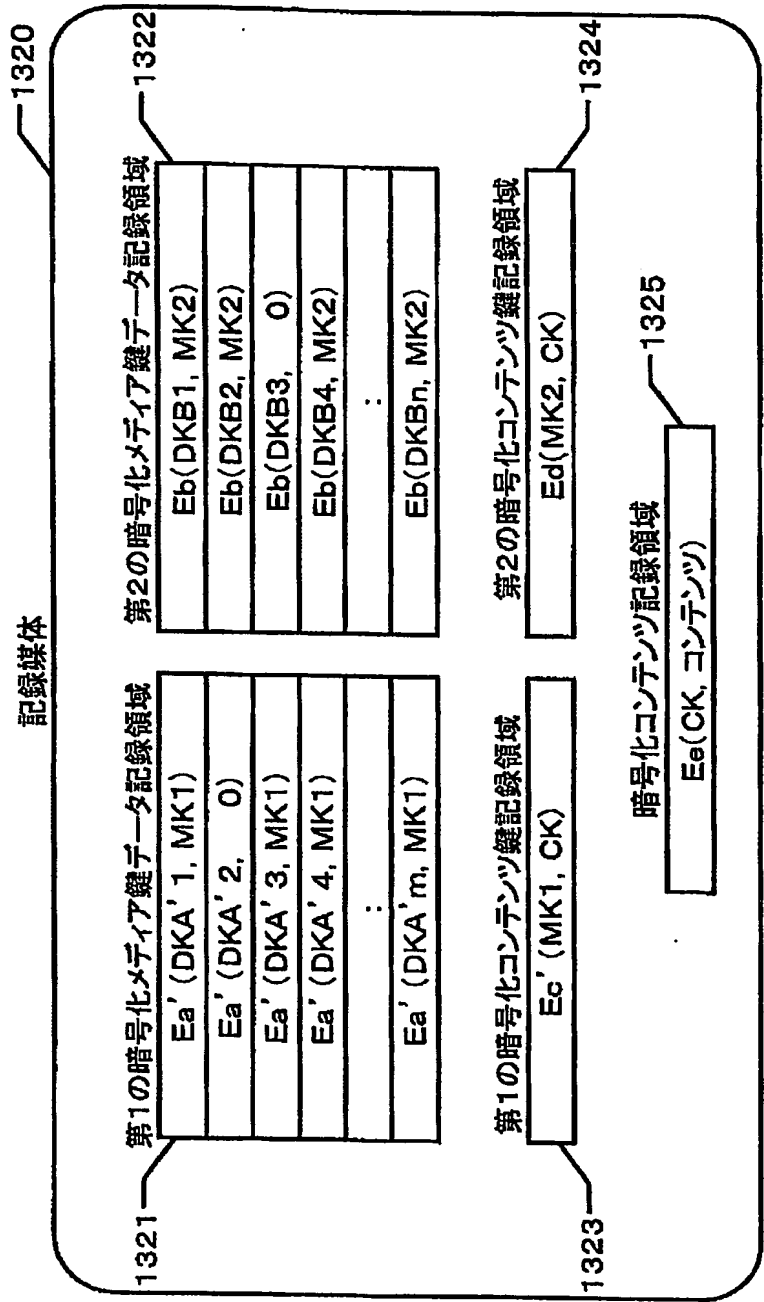


図19

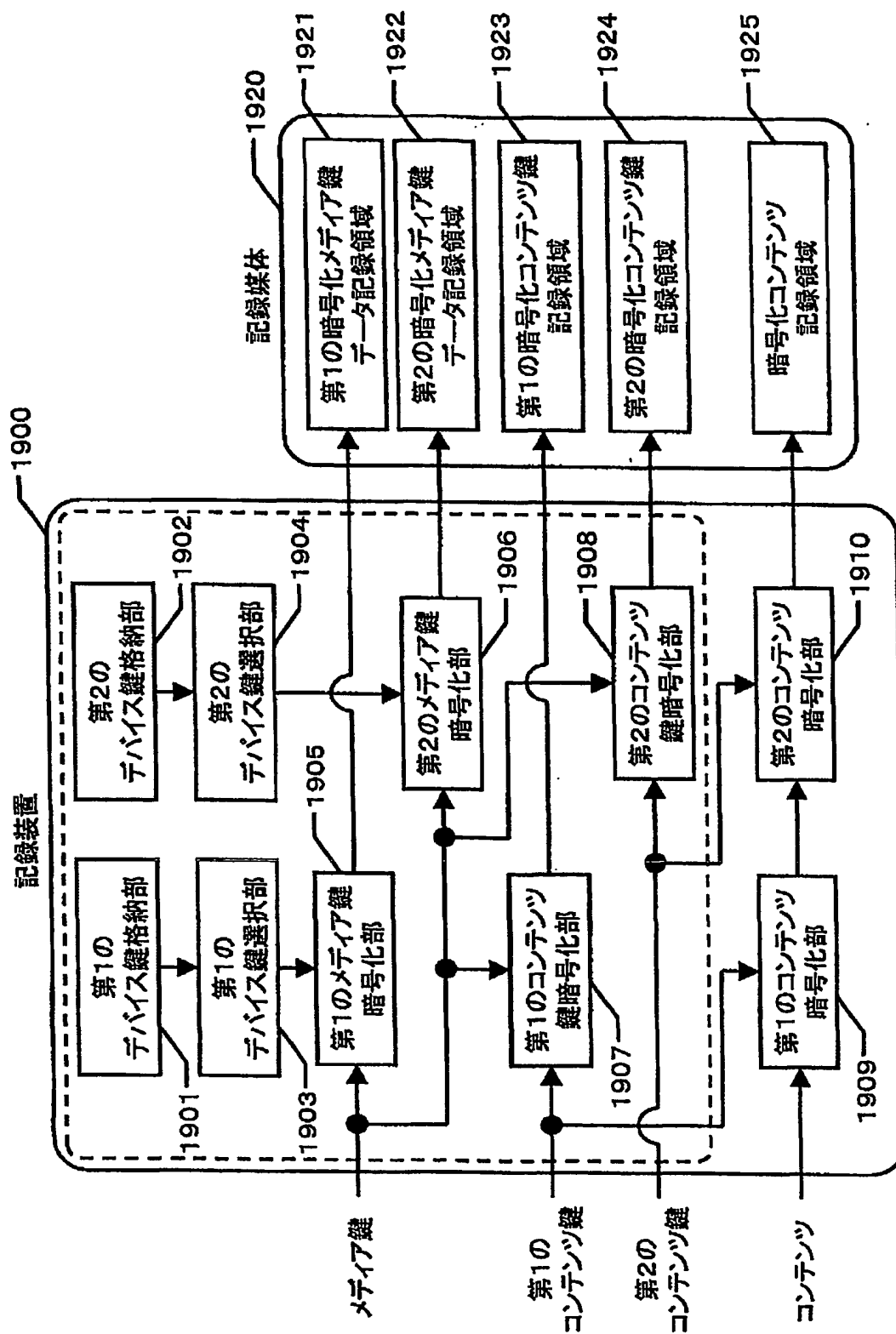


図20

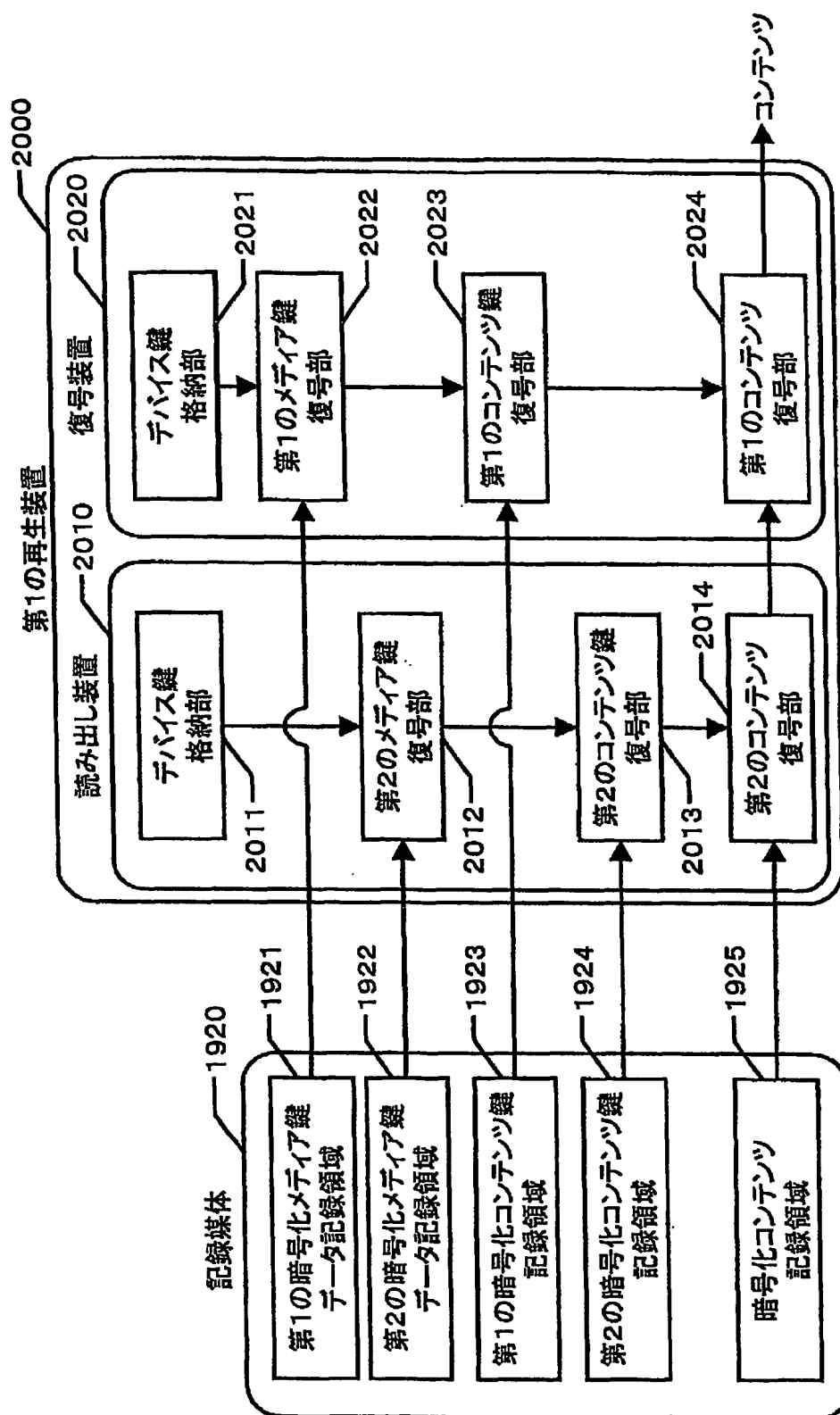


図21

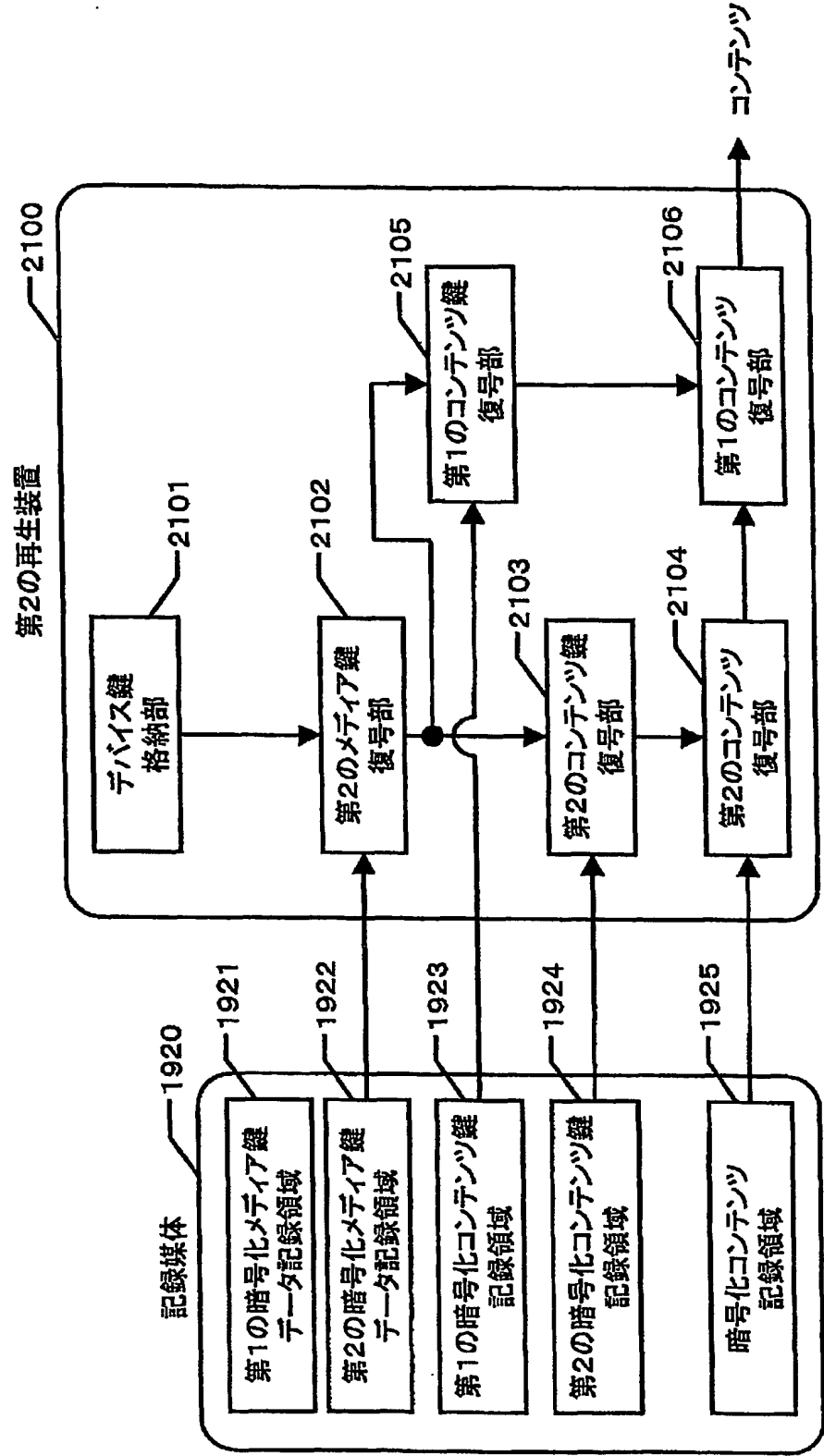


図22

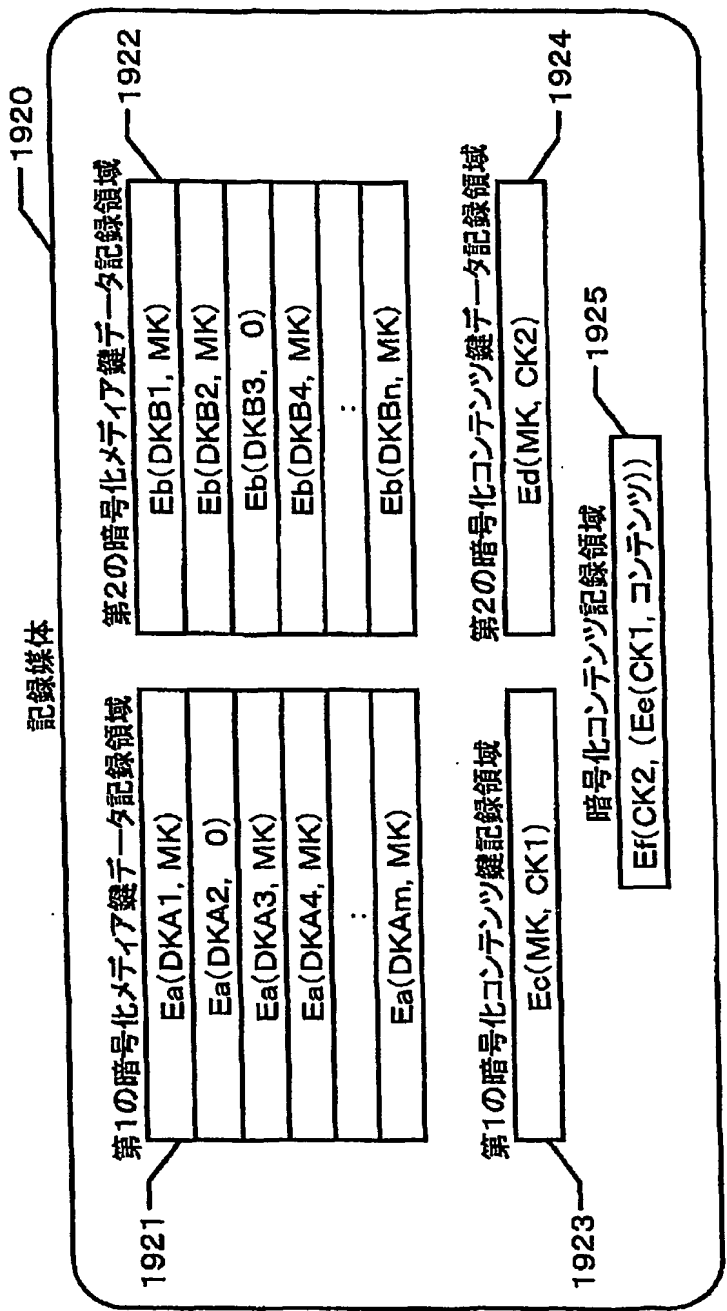


図23

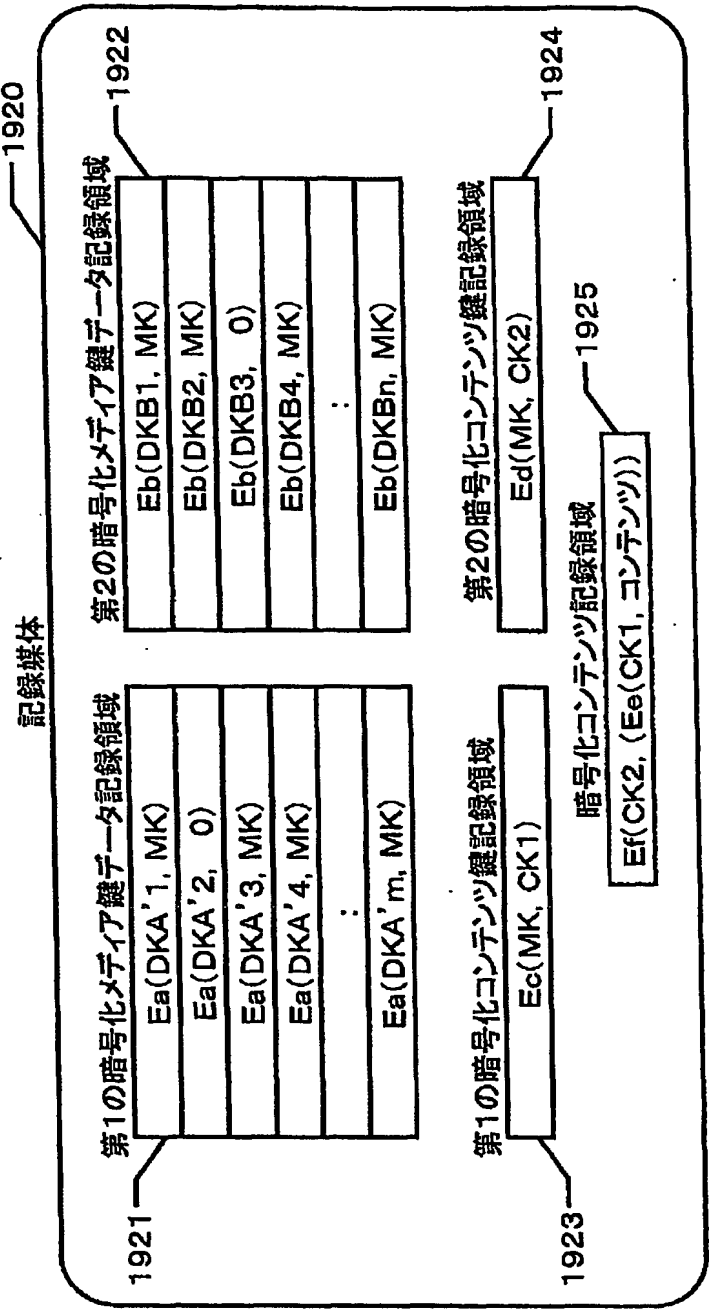




図24

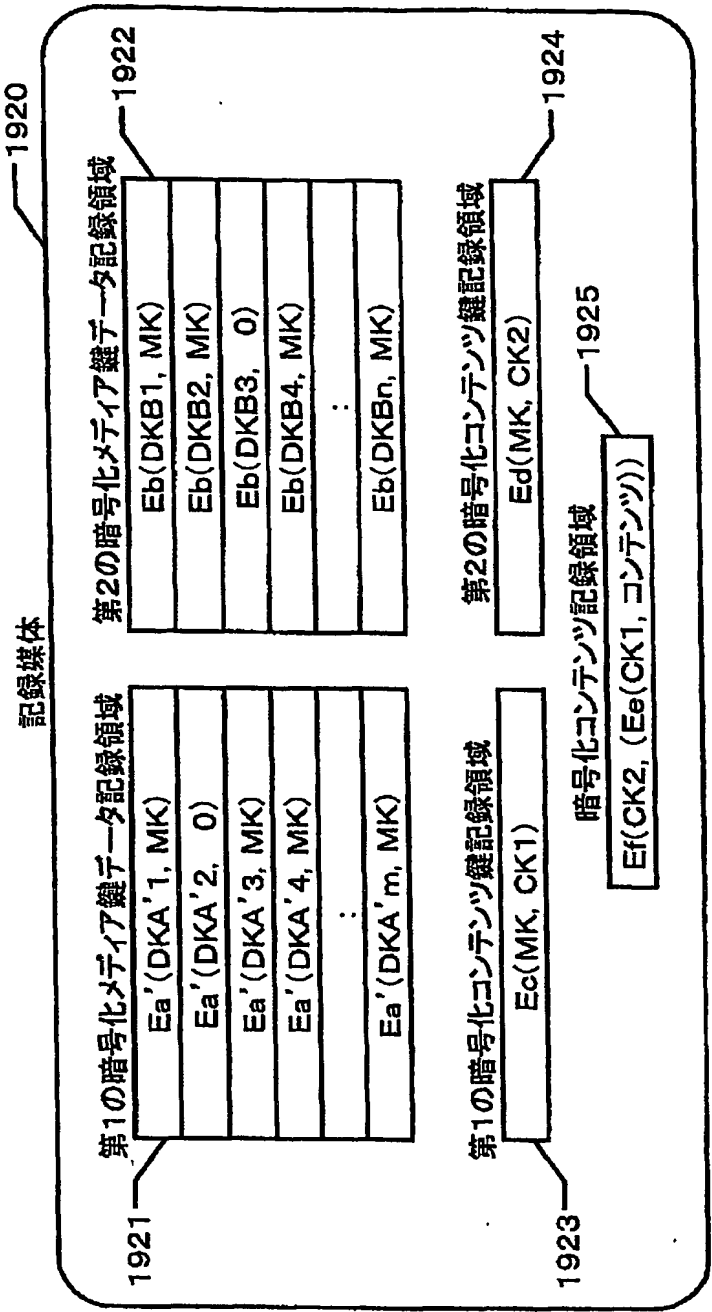


図25

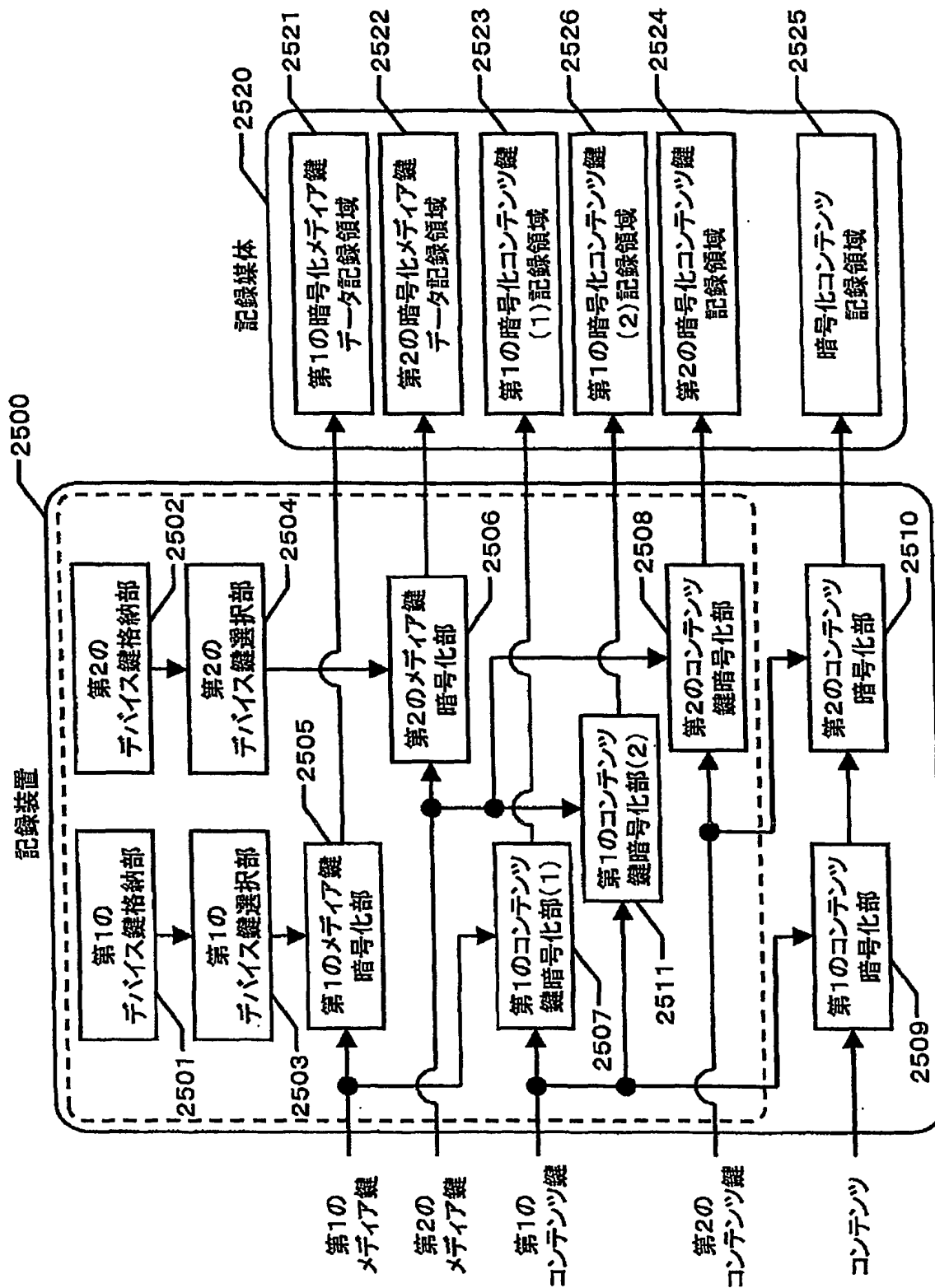


図26

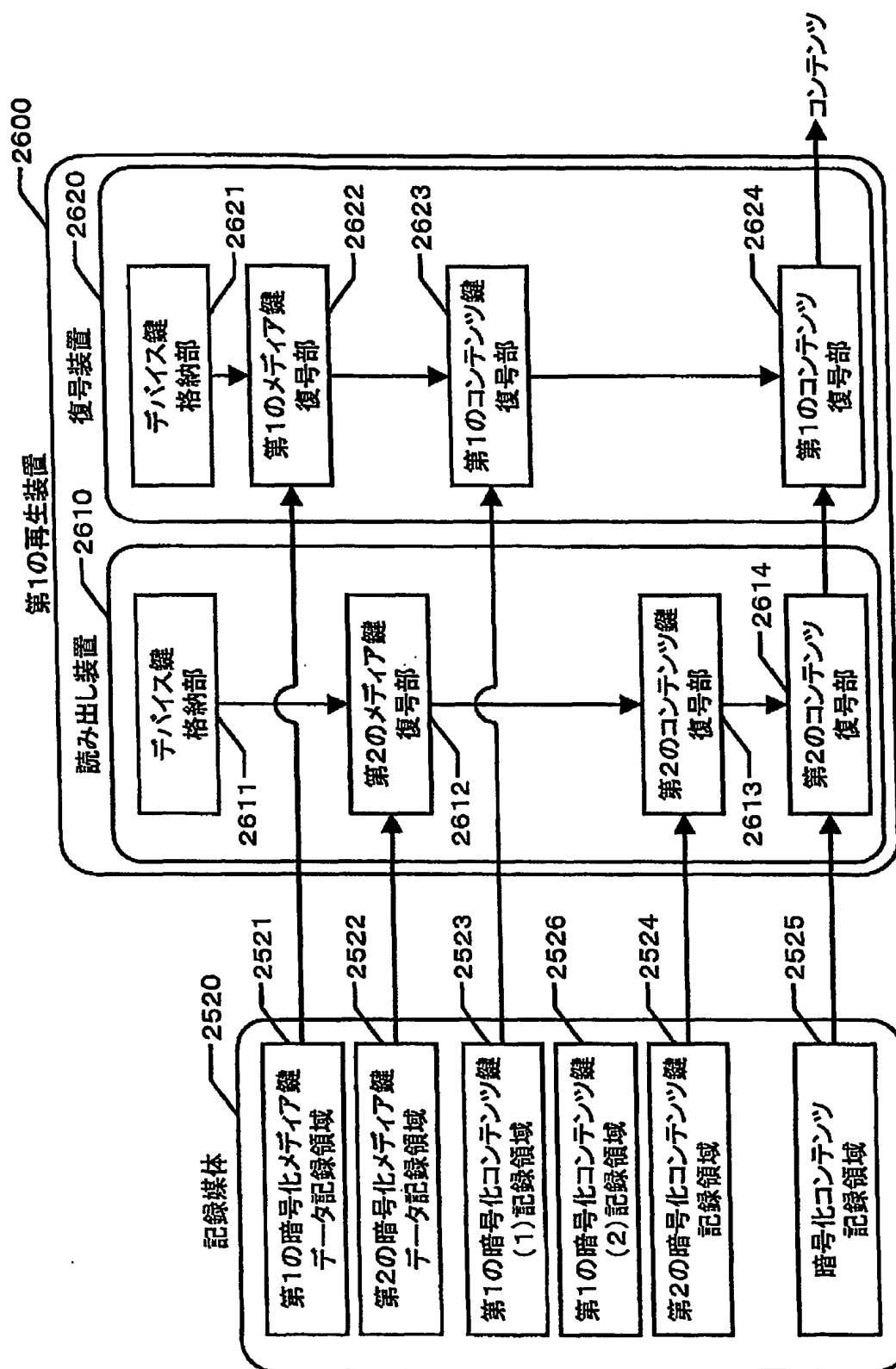


図27

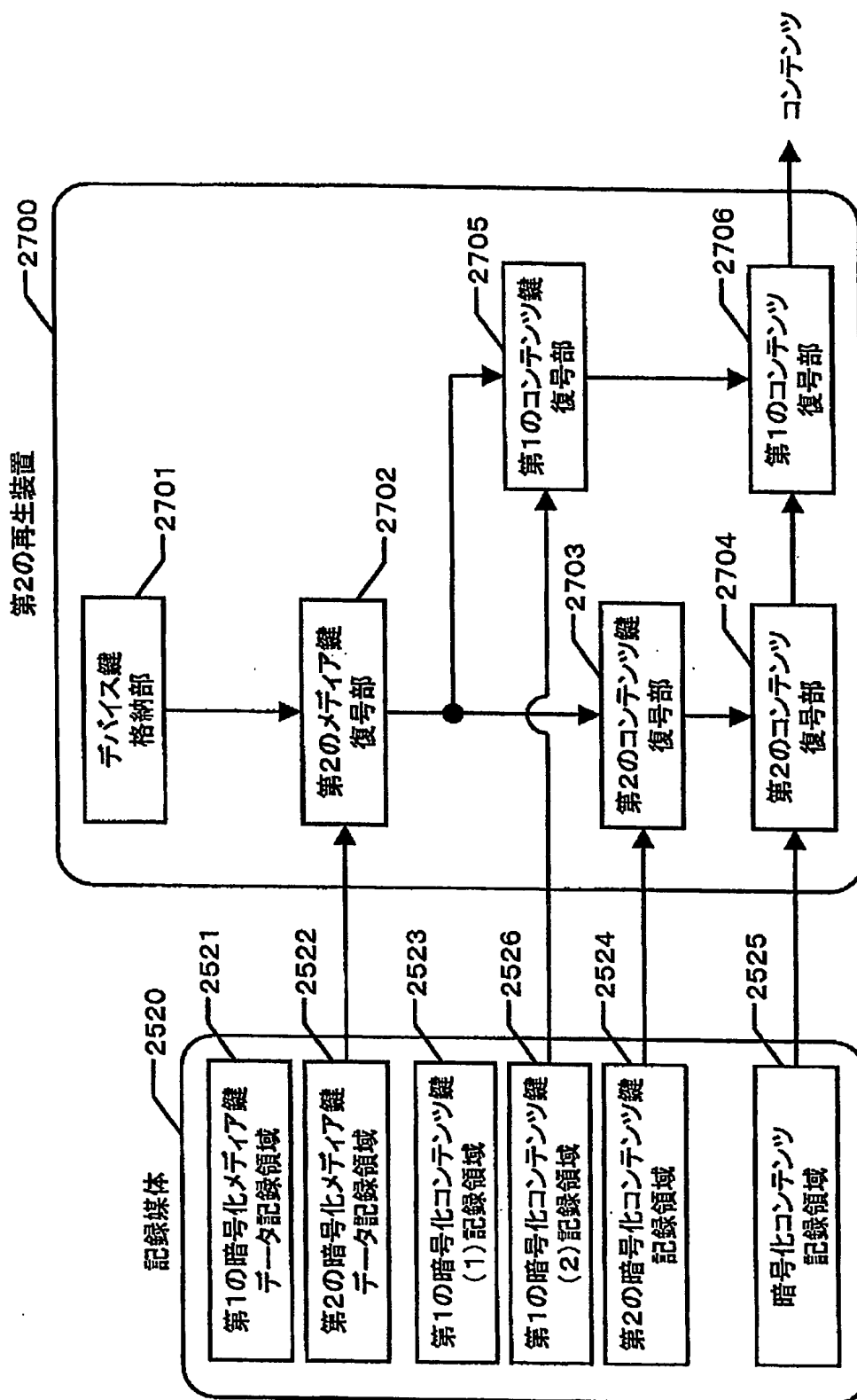


図28

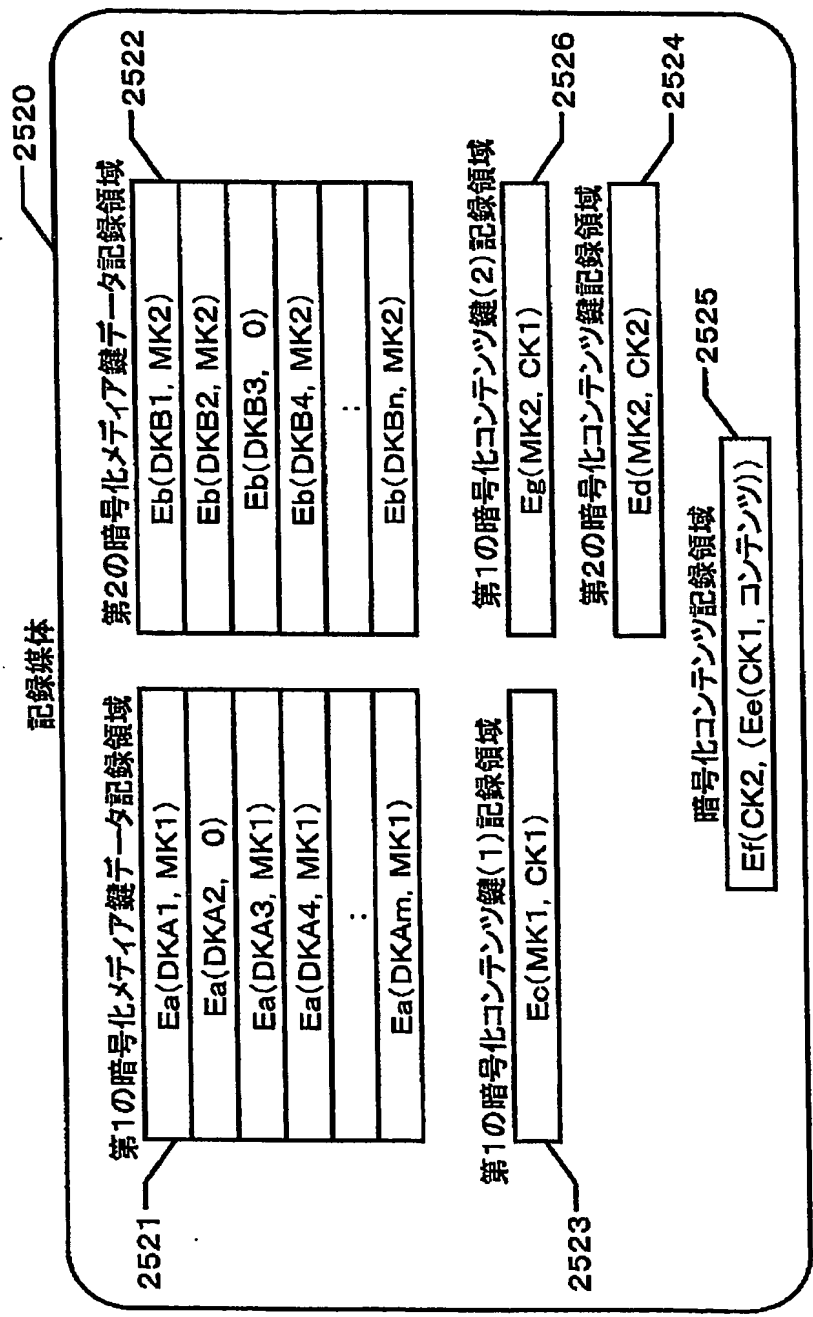


図29

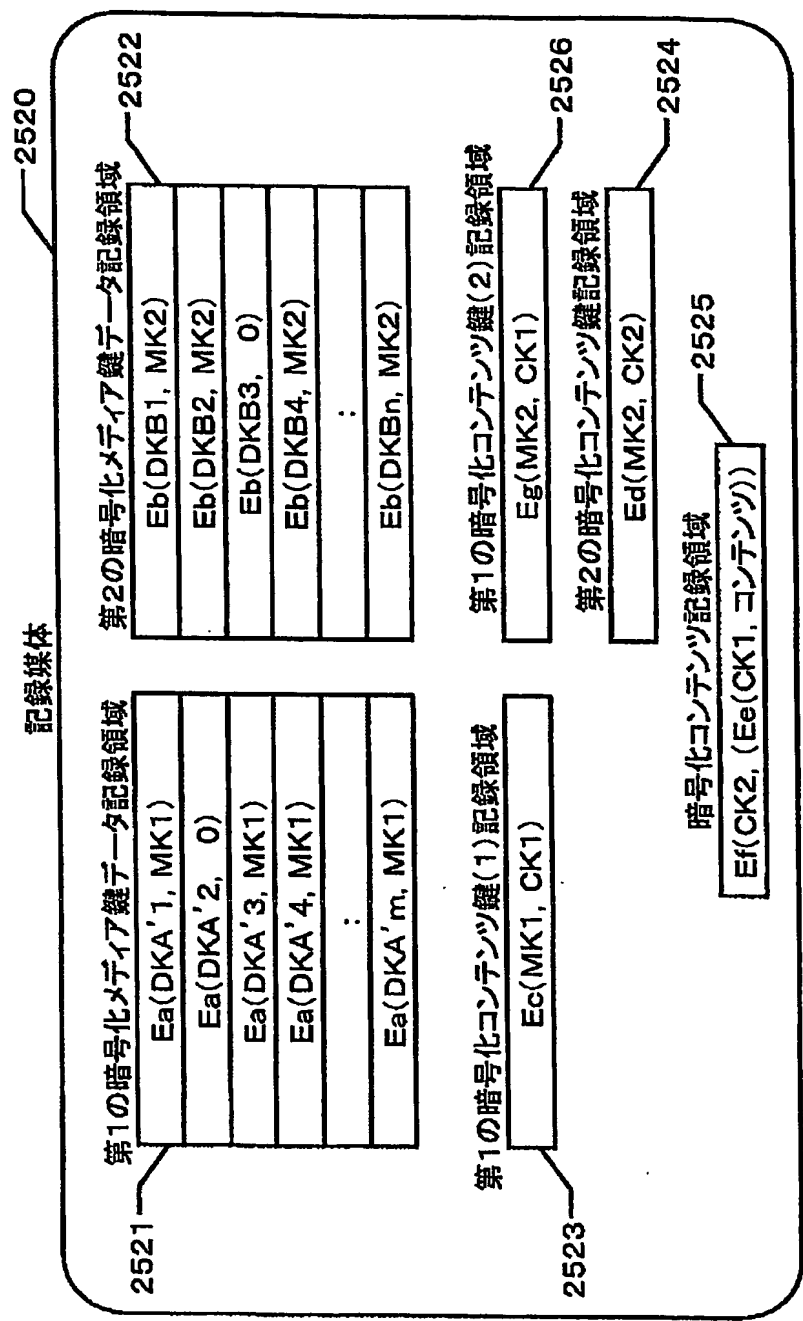


図30

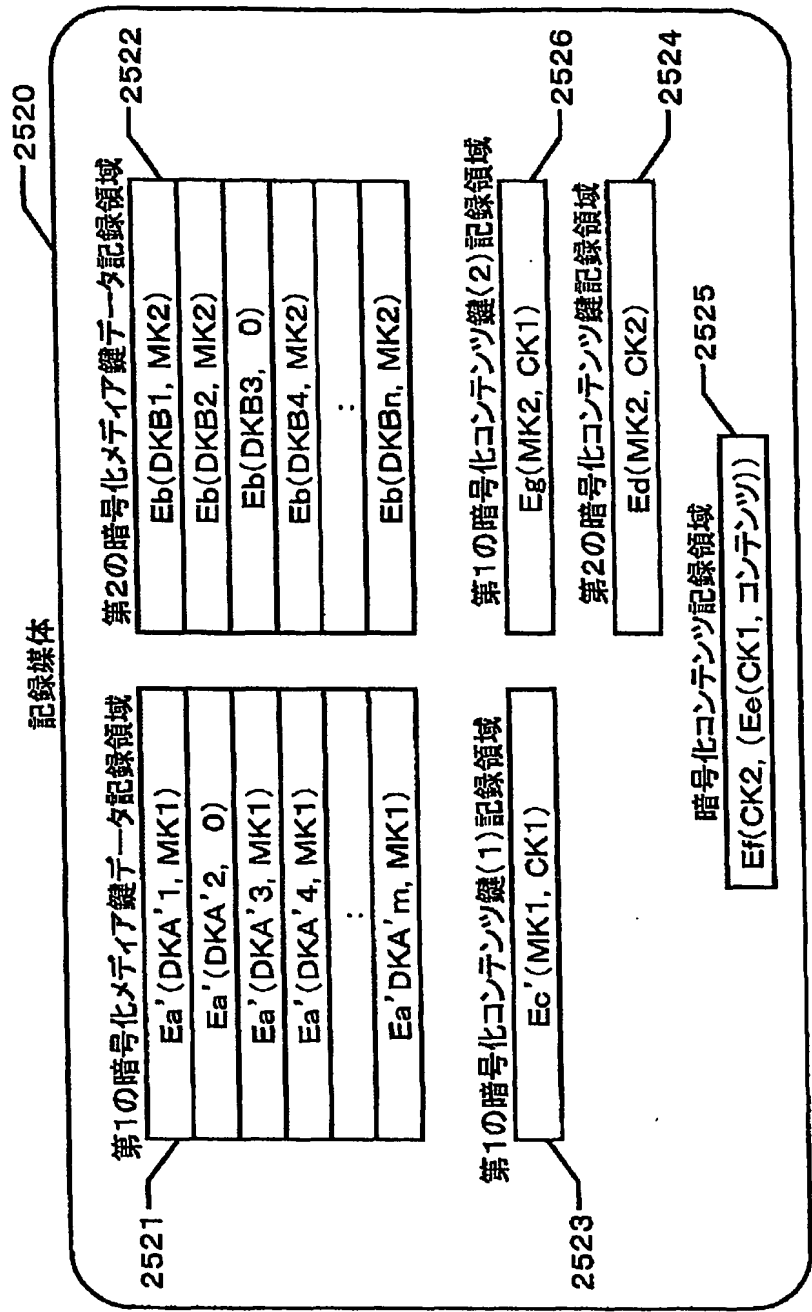


図31

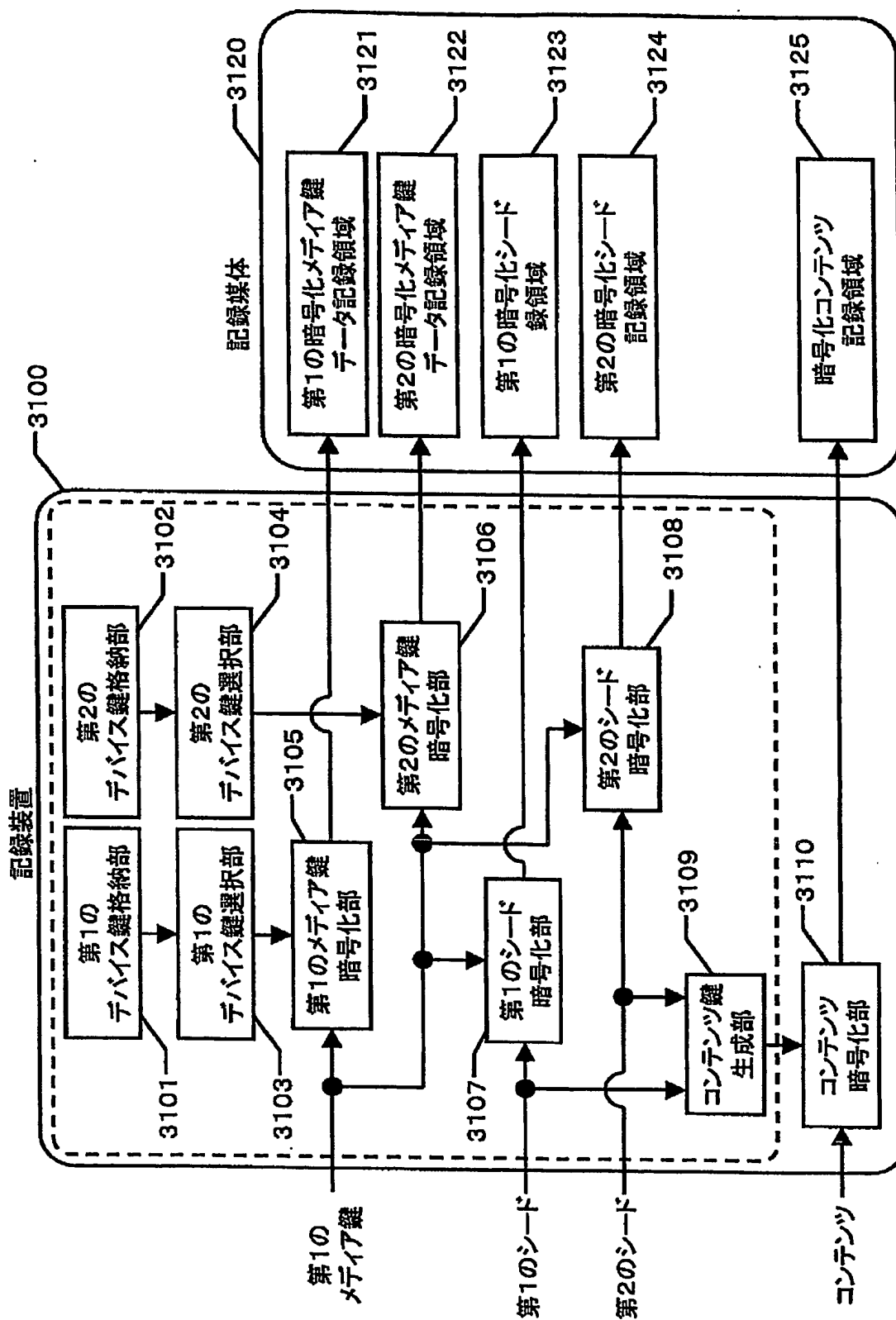


図32

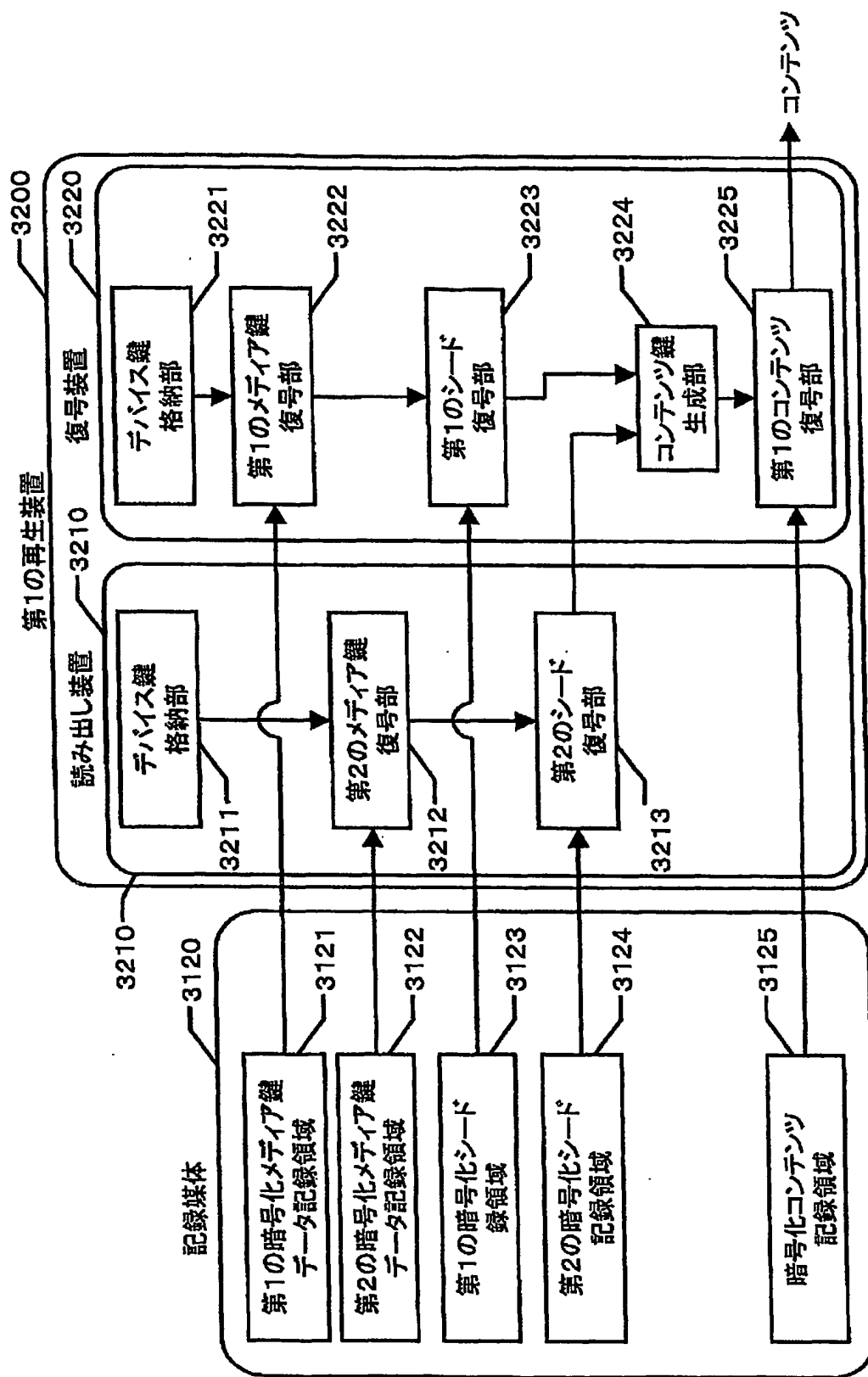


図33

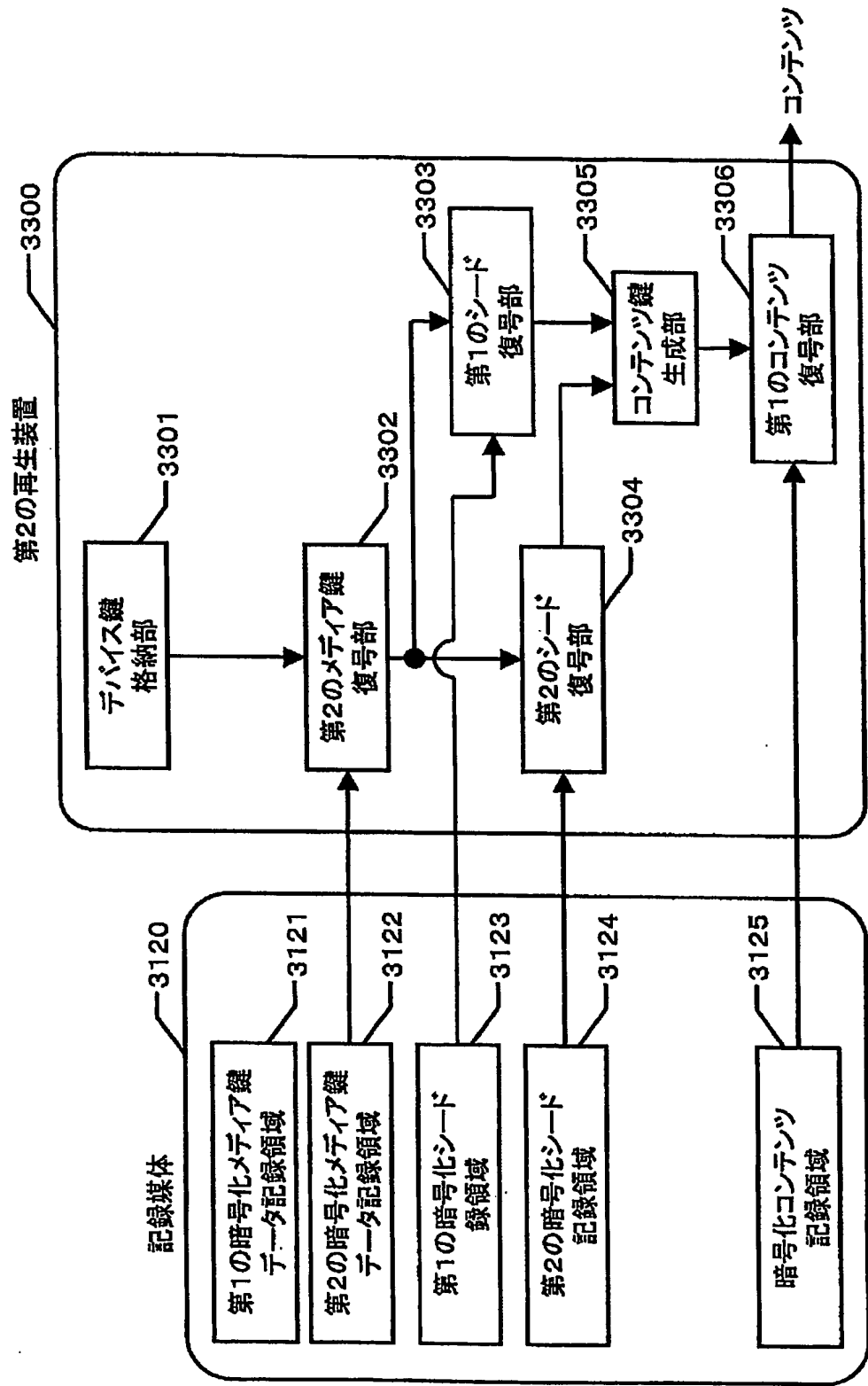


図34

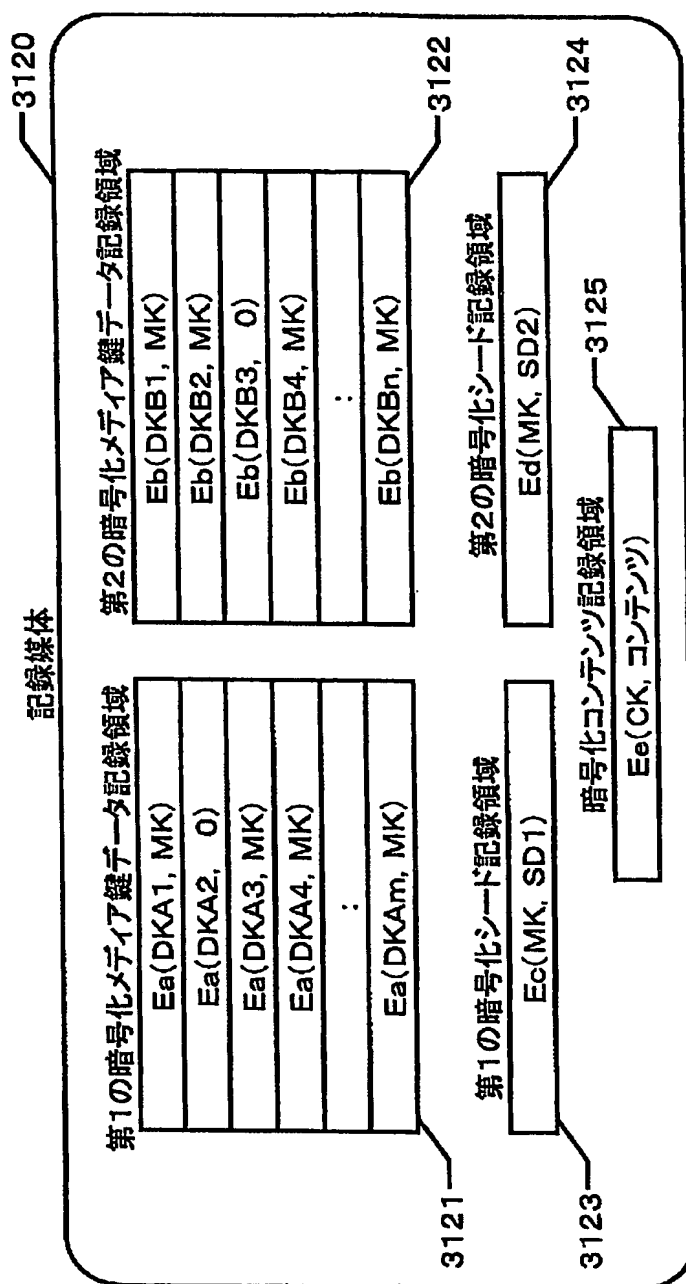


図35

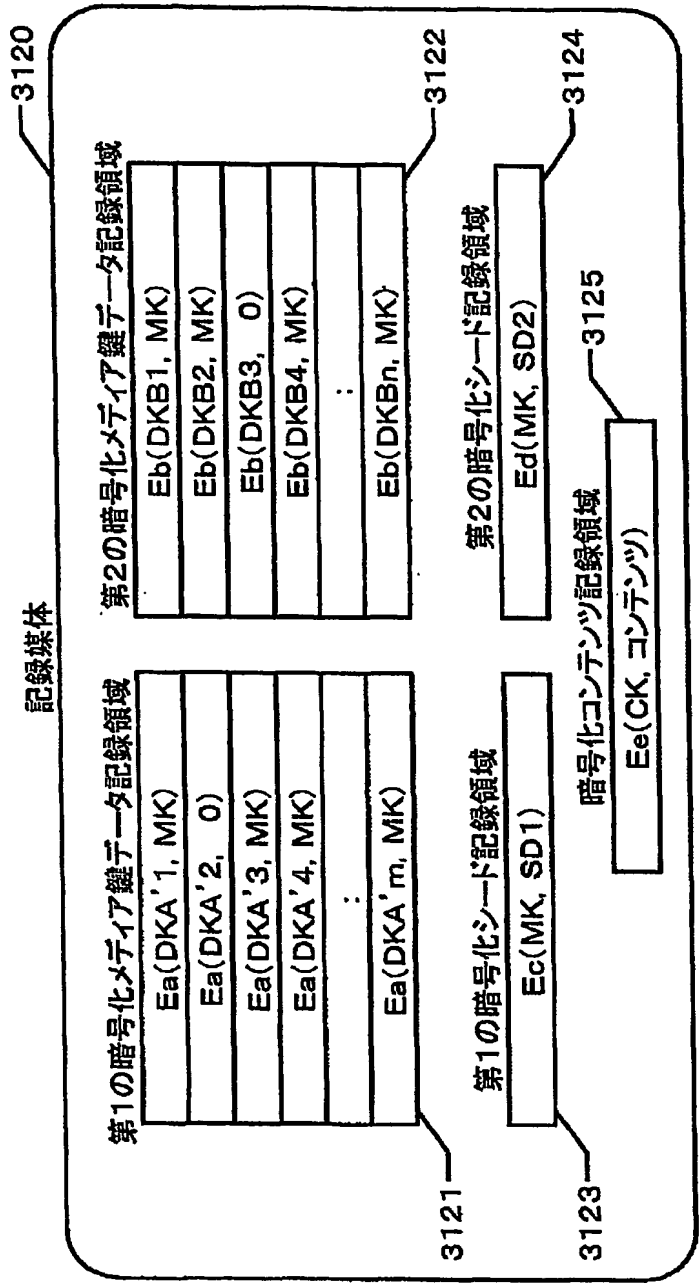


図36

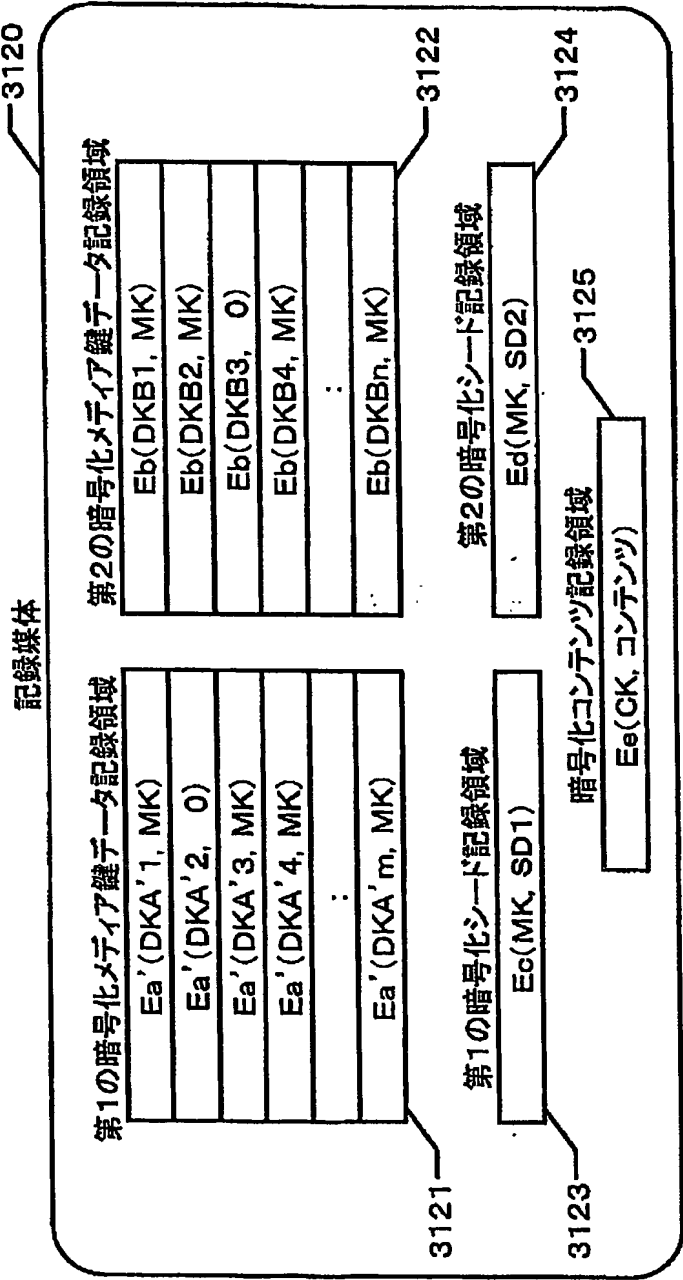


図37

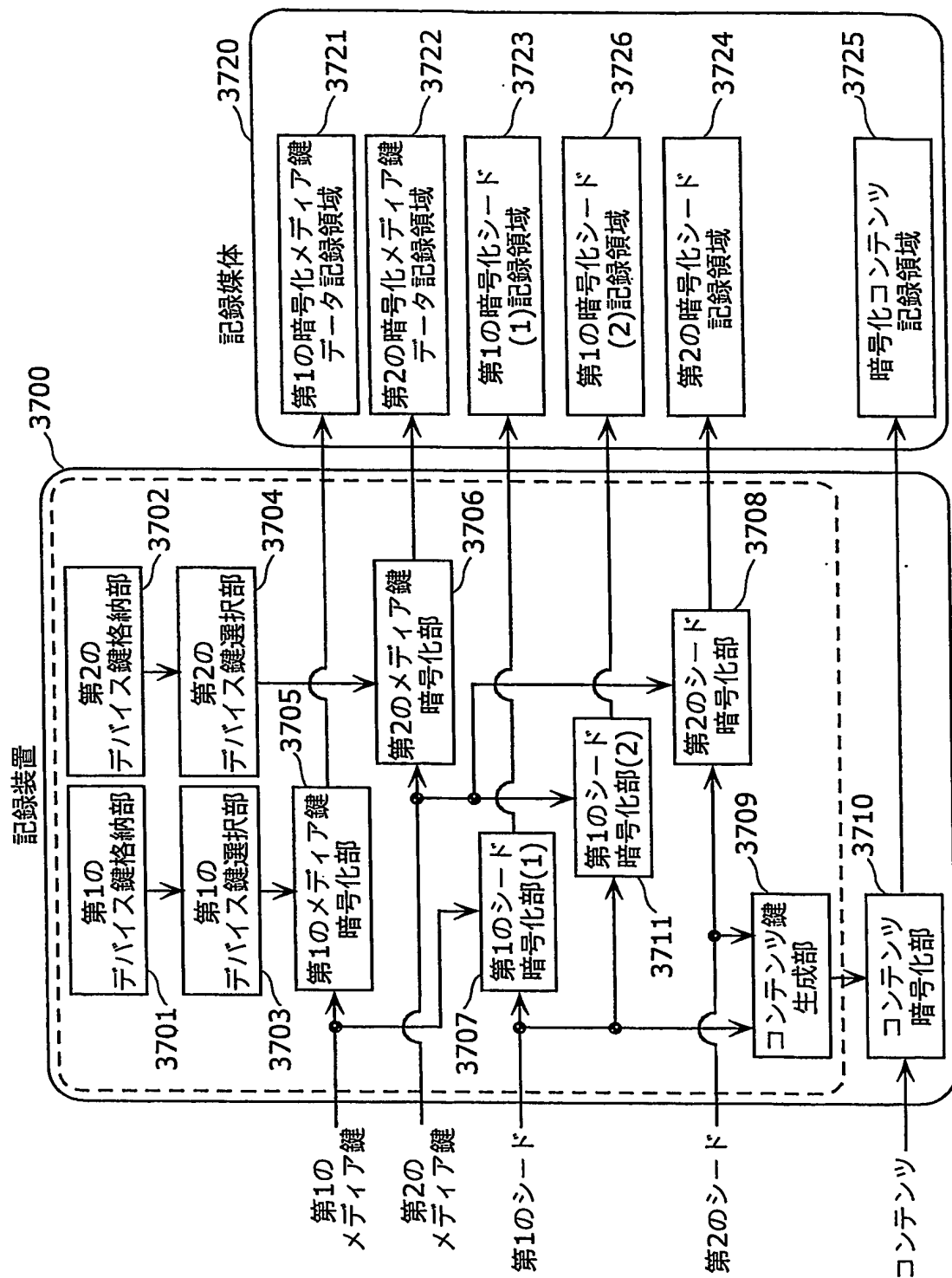


図38

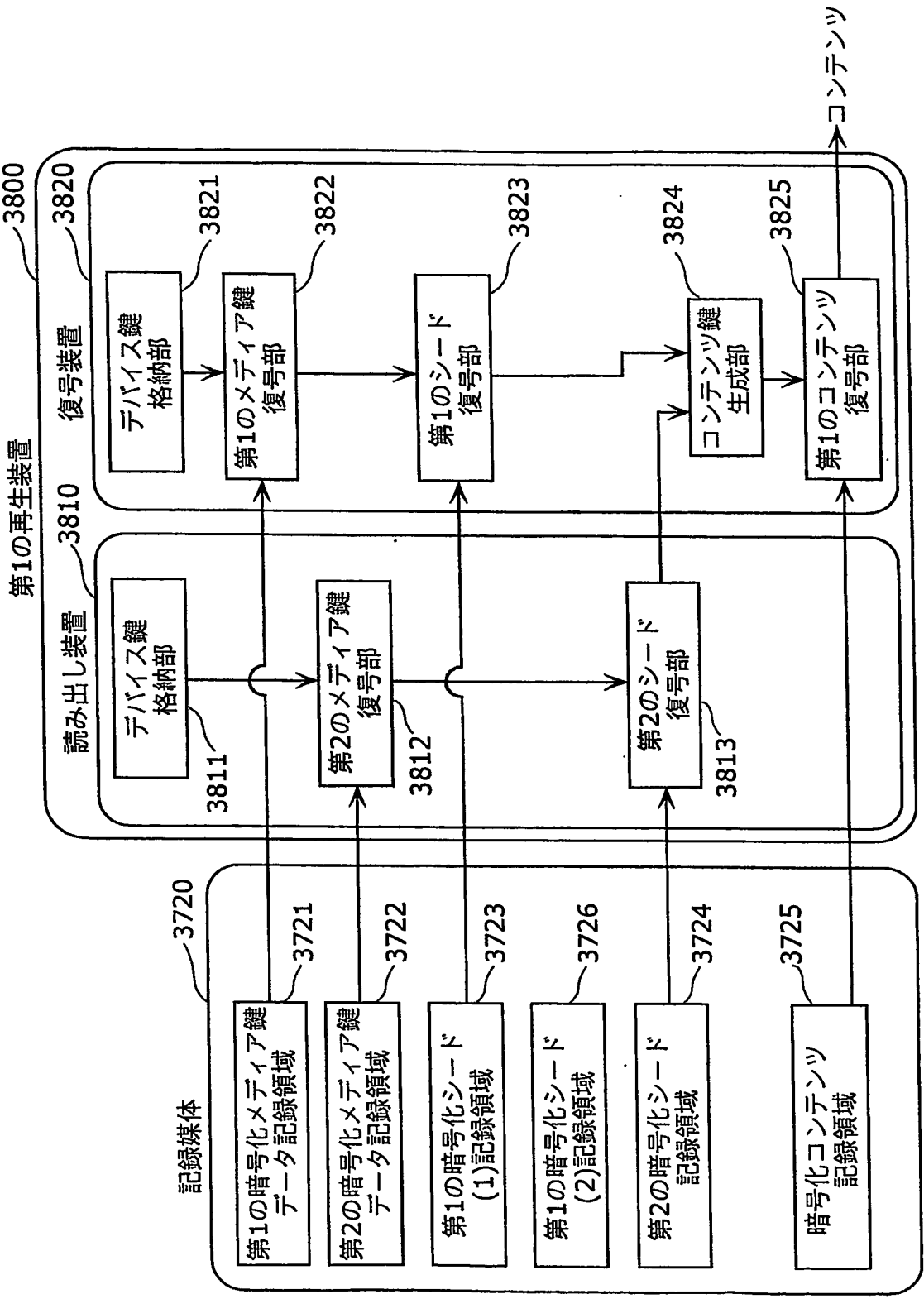


図39

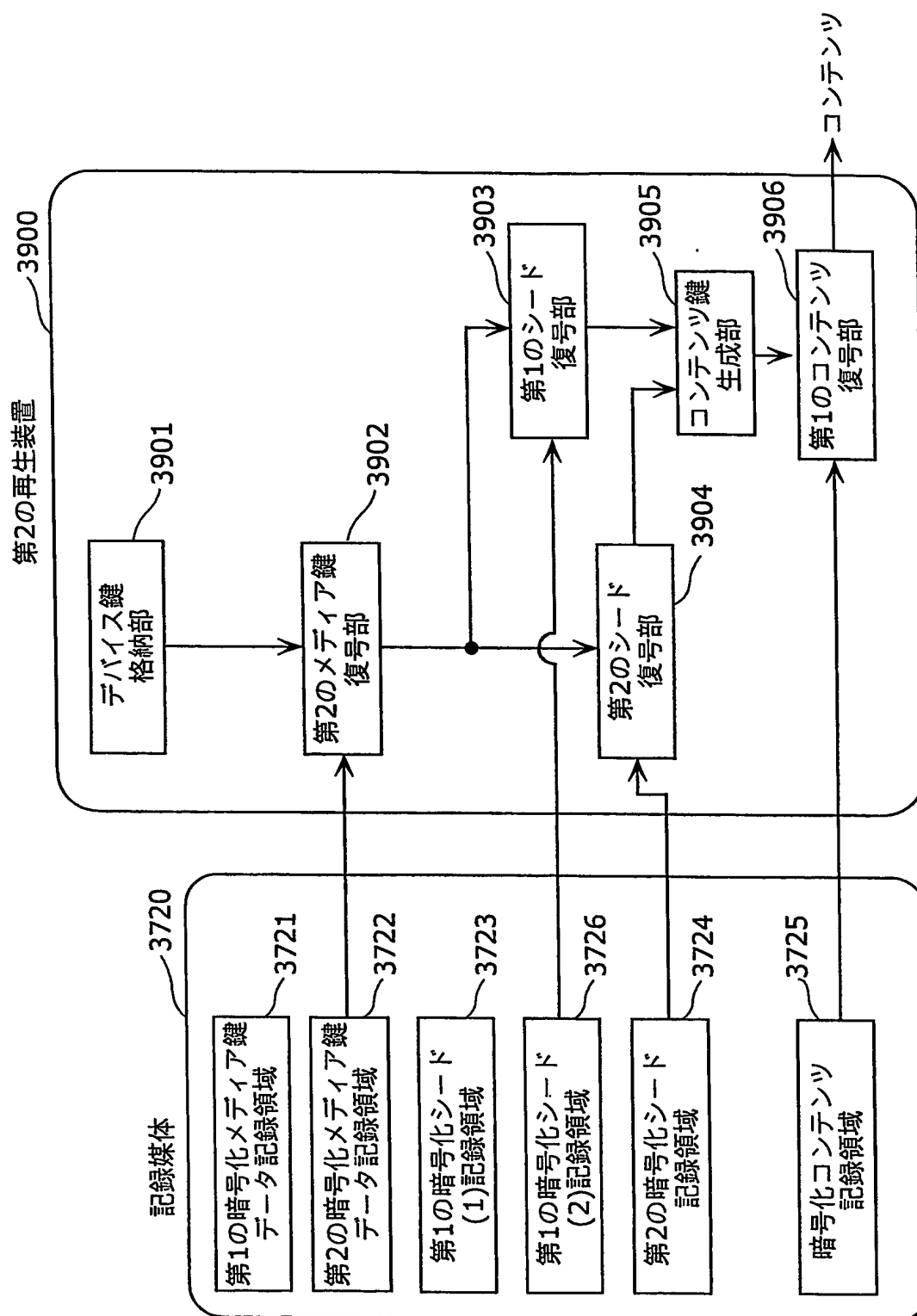


図40

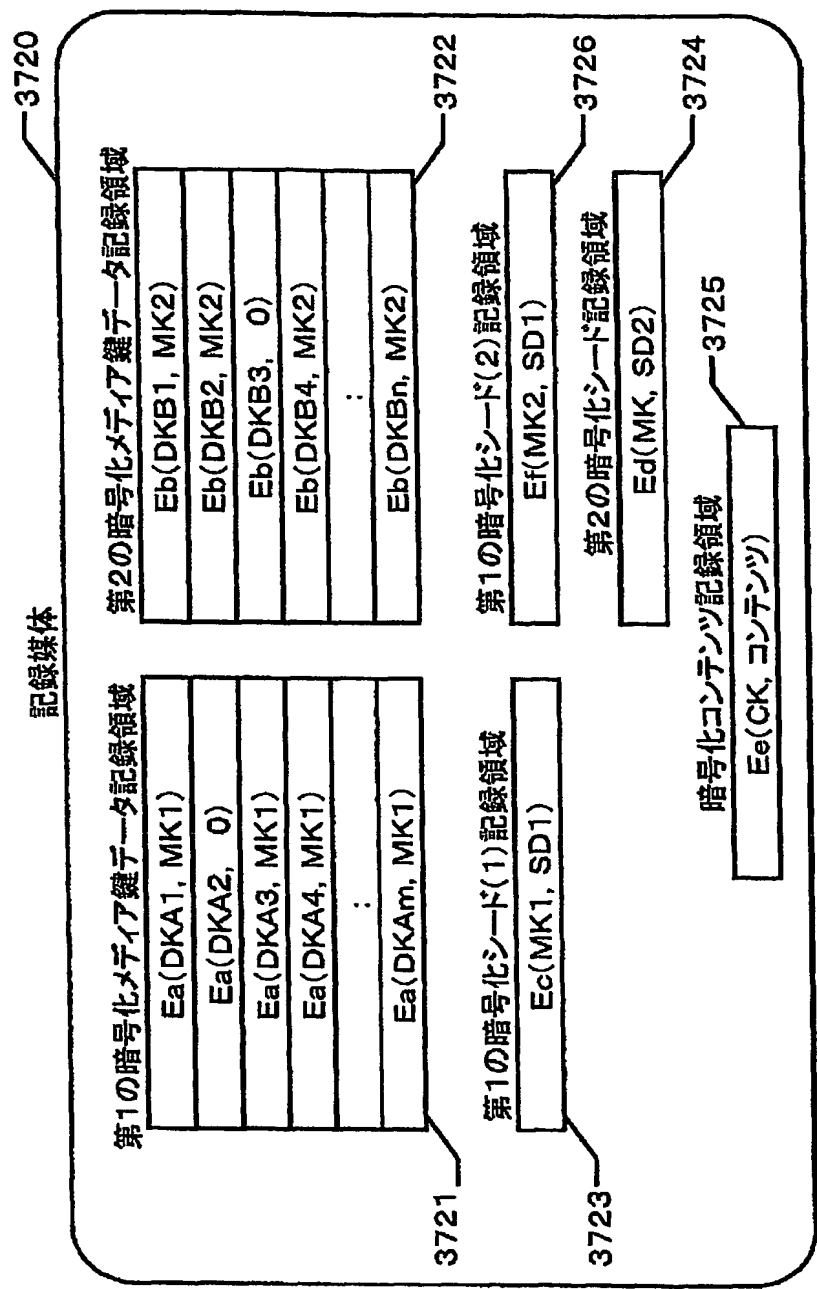


図41

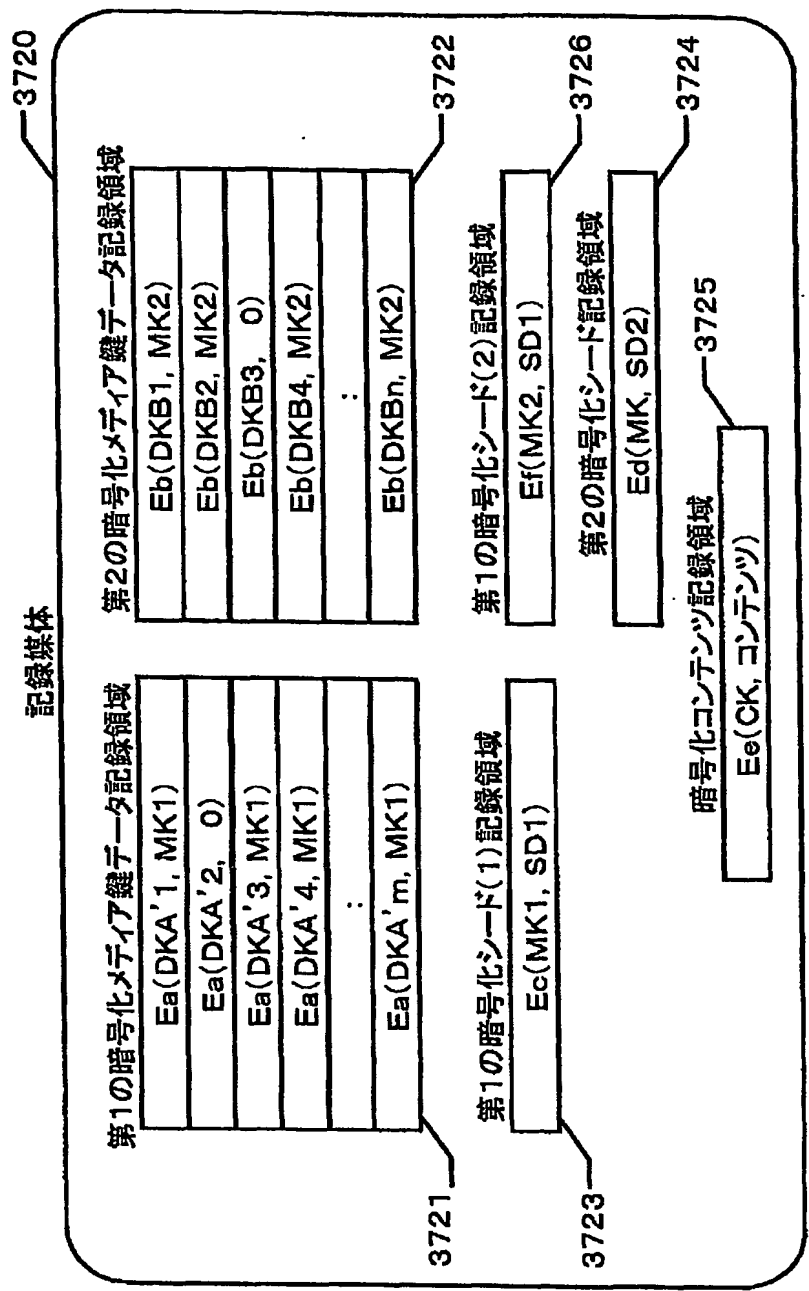
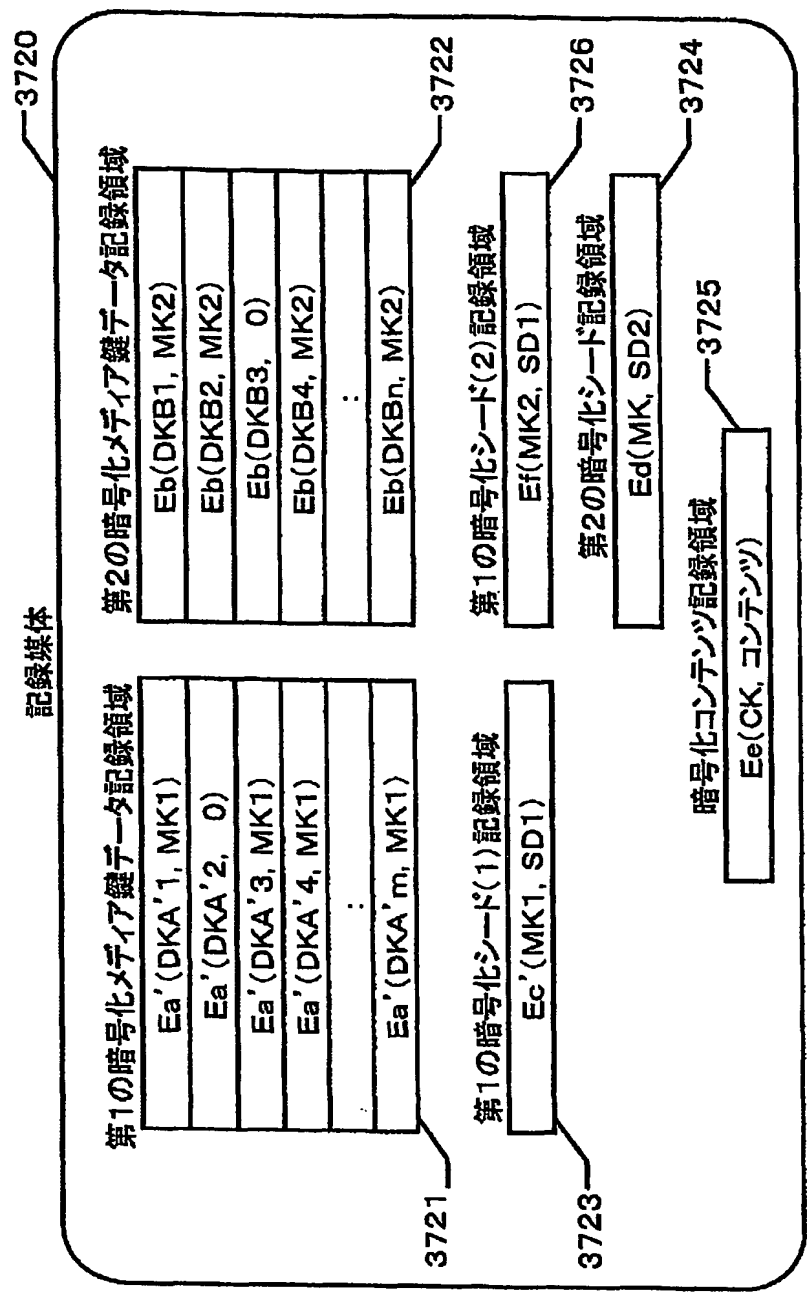


図42



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011303

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Makoto Tatebayashi, Toshiharu HARADA, Yoshihisa FUKUSHIMA, Hideyuki ISHIHARA, "Kiroku Media no Contents Hogo System", 2000 Nen The Institute of Electronics, Information and Communication Engineers Kiso · Kyokai Society Taikai Koen Ronbunshu, 07 September, 2000 (07.09.00), pages 367 to 368	1-34
Y	JP 2000-23137 A (Matsushita Electric Industrial Co., Ltd.), 21 January, 2000 (21.01.00), Full text; Figs. 1 to 6 & TW 416246 B & EP 969667 A & CN 1249621 A & SG 71930 A & AU 741900 A & US 6714649 B	1-34

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26 October, 2004 (26.10.04)

Date of mailing of the international search report
16 November, 2004 (16.11.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011303

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-181689 A (Sony Corp.), 12 July, 1996 (12.07.96), Par. Nos. [0025], [0028] to [0033], [0054] to [0067]; Figs. 1, 2, 7 & EP 710025 A & US 5721778 A & EP 996288 A & JP 2000-316144 A & JP 2003-46497 A & JP 2003-264550 A	6, 25-27

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	館林誠, 原田俊治, 福島能久, 石原秀志, “記録メディアのコンテンツ保護システム”, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 2000. 09. 07, p. 367-368	1-34
Y	JP 2000-23137 A (松下電器産業株式会社) 2000. 01. 21 全文, 図1-6 & TW 416246 B & EP 969667 A & CN 1249621 A & SG 71930 A & AU 741900 A & US 6714649 B	1-34

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリ

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

26. 10. 2004

国際調査報告の発送日

16.11.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 8-181689 A (ソニー株式会社) 1996. 07. 12 第【0025】段落, 第【0028】-【0033】段落, 第【0054】-【0067】段落, 図1, 2, 7 & EP 710025 A & US 5721778 A & EP 996288 A & JP 2000-316144 A & JP 2003-46497 A & JP 2003-264550 A	6, 25-27

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.